

Brought to you by:



# The eIDAS Regulation

for  
**dummies**<sup>®</sup>  
A Wiley Brand



- Explore the eIDAS Regulation
- 
- Understand electronic IDs and trust services
- 
- Discover ways to become compliant

nCipher Security  
Special Edition

By Jonathan Allin  
and Nick Pope  
with Faithe Wempen

# About nCipher Security

nCipher Security, an Entrust Datacard company, is a leader in the general-purpose hardware security module (HSM) market, empowering world-leading organizations by delivering trust, integrity and control to their business critical information and applications. Today's fast-moving digital environment enhances customer satisfaction, gives competitive advantage and improves operational efficiency – it also multiplies the security risks. Our cryptographic solutions secure emerging technologies such as cloud, IoT, blockchain, and digital payments and help meet new compliance mandates. We do this using our same proven technology that global organizations depend on today to protect against threats to their sensitive data, network communications and enterprise infrastructure. We deliver trust for your business critical applications, ensure the integrity of your data and put you in complete control – today, tomorrow, always. [www.ncipher.com](http://www.ncipher.com)



# The eIDAS Regulation

nCipher Security Special Edition

**By Jonathan Allin  
and Nick Pope**  
with Faithe Wempen

for  
**dummies**<sup>®</sup>  
A Wiley Brand

# The eIDAS Regulation For Dummies®, nCipher Security Special Edition

Published by: **John Wiley & Sons, Ltd.**, The Atrium, Southern Gate Chichester, West Sussex,  
[www.wiley.com](http://www.wiley.com)

© 2020 by John Wiley & Sons, Ltd., Chichester, West Sussex

*Registered Office*

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ,  
United Kingdom

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted by the UK Copyright, Designs and Patents Act 1988, without the prior written permission of the Publisher. For information about how to apply for permission to reuse the copyright material in this book, please see our website <http://www.wiley.com/go/permissions>.

**Trademarks:** Wiley, For Dummies, the Dummies Man logo, The Dummies Way, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. nCipher and the nCipher logo are trademarks of nCipher Security, LLC. All other trademarks are the property of their respective owners. John Wiley & Sons, Ltd., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: WHILE THE PUBLISHER AND AUTHOR HAVE USED THEIR BEST EFFORTS IN PREPARING THIS BOOK, THEY MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS BOOK AND SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IT IS SOLD ON THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING PROFESSIONAL SERVICES AND NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. IF PROFESSIONAL ADVICE OR OTHER EXPERT ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL SHOULD BE SOUGHT.

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact [info@dummies.biz](mailto:info@dummies.biz), or visit [www.wiley.com/go/custompub](http://www.wiley.com/go/custompub). For information about licensing the *For Dummies* brand for products or services, contact [BrandedRights&Licenses@Wiley.com](mailto:BrandedRights&Licenses@Wiley.com).

ISBN 978-1-119-65222-9 (pbk); ISBN 978-1-119-65223-6 (ebk)

Printed in Great Britain

10 9 8 7 6 5 4 3 2 1

## Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

**Project Editor:** Jennifer Bingham  
**Acquisitions Editor:** Katie Mohr  
**Editorial Manager:** Rev Mengle

**Business Development  
Representative:** Frazier Hossack  
**Production Editor:**  
Mohammed Zafar Ali

# Table of contents

INTRODUCTION .....	1
How This Book Is Organised .....	1
Chapter 1: What Is eIDAS? .....	2
Chapter 2: Electronic IDs and Trust Services .....	2
Chapter 3: Electronic Signatures: Click on the Dotted Line .....	2
Chapter 4: HSMs in the eIDAS World.....	3
Chapter 5: Ten Ways nCipher Security Can Help You .....	3
Appendix: Further Information .....	3
Foolish Assumptions.....	3
Icons Used in This Book.....	4
Where to Go from Here.....	4
<b>CHAPTER 1: What Is eIDAS? .....</b>	<b>5</b>
Stepping Back in Time: Before eIDAS .....	6
Understanding eIDAS.....	7
The eIDAS vision.....	9
Who and what are affected?.....	9
What the Regulation contains .....	11
Exploring the Role of Identity and Trust Services.....	11
eIDAS e-Identity (eID) services.....	12
eIDAS trust services .....	13
The link between eIDAS eID and trust services.....	13
How identity and trust services work together .....	14
Figuring Out the Current State of Affairs.....	15
<b>CHAPTER 2: Electronic IDs and Trust Services .....</b>	<b>19</b>
No Paper, Please! Electronic IDs.....	20
Existing eIDs in Member States.....	20
eIDs under eIDAS .....	21
Putting Your Trust in Trust Services.....	22
Certificates and public keys .....	23
Time-stamping .....	24
Links between eID and Trust Services .....	25
Keeping Everyone Consistent: TSP Standards .....	26
ETSI general standards.....	27
ETSI standards for specific TSP types .....	27

Knowing Whom to Trust: Qualification and Auditing .....	28
Qualified TSP status.....	29
TSP auditing.....	30
Trust us! National lists of qualified TSPs .....	31
<b>CHAPTER 3: Electronic Signatures: Click on the Dotted Line .....</b>	<b>33</b>
Discovering Uses for Electronic Signatures.....	34
Exploring Electronic Signatures .....	35
Gaining the (Electronic) Seal of Approval .....	37
Understanding Essential Seal and Signature Standards .....	38
Smart Card Signing: The Old Way .....	39
Signing in the Cloud: The New Way .....	40
Four elements for trustworthy cloud signing.....	42
Cloud signing standards .....	43
Use of HSMs for Electronic Signatures and Seals.....	46
<b>CHAPTER 4: HSMs in the eIDAS World .....</b>	<b>47</b>
Recognising Why You Might Need an HSM.....	48
Signing certificates and time stamps.....	48
Document signing in the cloud .....	48
Document sealing.....	49
Knowing What to Look for in an HSM.....	49
Check the certification.....	49
Search for scalability.....	50
Bend toward flexibility .....	51
Establish what can be protected.....	51
Find out about running apps securely .....	52
Sorting Out the Standards: Three Examples.....	52
Signing certificates and time stamps.....	52
Document signing in the cloud .....	53
Document sealing.....	53
Choosing Your HSM Provider .....	54
<b>CHAPTER 5: Ten Ways nCipher Can Help You .....</b>	<b>57</b>
<b>APPENDIX: FURTHER INFORMATION .....</b>	<b>65</b>

# Introduction

Everyone agrees that trading electronically, through a secure and trusted service infrastructure, is the way of the future. For example, most people have used the Internet to buy things, and more and more trade depends on documents being signed electronically.

All of these transactions depend on infrastructures of trust services and increasingly, citizens, governments, and businesses are making use of these infrastructures. That's the good news.

The bad news is that, at least in the EU, it's been a real Tower of Babel situation until lately. Every country has had some sort of trust service infrastructure, but many of them haven't been able to recognise each other, particular when it comes to using electronic signatures. For example, a document (such as a contract) electronically signed in one person's home country could not be verified as being legally valid when read electronically in another European country.



REMEMBER

The main point of having the EU is to allow for seamless cross-border activities, so having incompatible electronic trust service infrastructures has been an important obstacle to overcome.

Fixing this problem was the objective of a 2014 EU Regulation on Electronic Identification and Trust Services (commonly called eIDAS), which began taking effect in EU Member States in 2016. This Regulation creates consistent standards across the EU for electronic identities, authentication, and signatures, so that no matter which country a citizen is in, and which governments and businesses she is working with, she won't have any compatibility issues.

In this handy little book, we explain eIDAS and its consequences in simple, easy-to-understand terms, so even those with no prior knowledge can make sense of it all.

## How This Book Is Organised

As with other *For Dummies* books, this book doesn't just assume that you'll begin on page one and read straight through to the end. Each chapter is written to stand alone, with enough contextual information provided so that you can understand the content.

## Chapter 1: What Is eIDAS?

Chapter 1 explains the history and motivations for the 1999 Signature Directive, which was eIDAS's predecessor, and how it worked in some ways and fell short in others. This sets the stage for explaining how the eIDAS Regulation replaces the Directive and improves the adoption of trustworthy electronic services for all.

Also in Chapter 1, you'll learn the basics of the eIDAS Regulation as it was passed in 2014, including what it's expected to achieve and what kinds of businesses and government agencies are affected. This chapter also outlines the current state of affairs in terms of compliance requirements. Whereas the Regulation itself is complete and final, there are still countless small details being worked out about *how* its objectives will be achieved.

## Chapter 2: Electronic IDs and Trust Services

Chapter 2 looks at the two main aspects of eIDAS: electronic identities, and trust services for authentication and signatures. Firstly the chapter explains the benefits of electronic identification and describes how eIDAS provides a bridge enabling EU countries to recognise each other's electronic IDs. You'll learn about the three assurance levels for electronic identification under eIDAS (low, substantial, and high), and the requirements for each.

Secondly this chapter explains trust services, the trust service providers (TSPs) that supply them, the standards to which TSPs are held, and the way TSPs are qualified and audited to make sure they are trustworthy.

## Chapter 3: Electronic Signatures: Click on the Dotted Line

In Chapter 3, we'll explore the field of electronic signatures, which is exploding in popularity across the EU and around the world. You'll find out what electronic signatures are good for, and what standards are in place to make sure an electronic signature can be trusted. You'll learn about the two types of electronic signatures (advanced and qualified), and when each type is appropriate. You'll also find out about a new variant of electronic signatures called a seal. These seals can be applied to documents from companies and other organisations, as opposed to electronic signatures which are applied by individuals.



This chapter also compares the old-technology way of signing (with smart cards) to the newer-technology way (signing in the cloud from personal mobile devices), both in how they work and what standards apply to them.

## Chapter 4: HSMs in the eIDAS World

Hardware Security Modules (HSMs) are important, providing the root of trust for the trust service infrastructures. Chapter 4 delves into their use under eIDAS, and here you'll find out why your organisation might need an HSM, such as for signing certificates, time stamps, or documents in the cloud, or for document sealing. You'll also find out what to look for when shopping around for an HSM, including features such as certification of compliance (that's the big one!), scalability, flexibility, and capabilities such as running applications within the HSM and interfacing with your existing applications.

## Chapter 5: Ten Ways nCipher Security Can Help You

Is your organisation ready for eIDAS? In Chapter 5, you'll find ten ways that nCipher Security can assist companies like yours, with advice and consultancy, commitment to the eIDAS standards, HSM certification compliance, qualified signature creation devices, and much more.

## Appendix: Further Information

Sometimes the devil is in the detail. This short appendix contains additional information that you may find helpful to reference, including the current timetable for implementing eIDAS, a framework of standards, and relevant information published online.

## Foolish Assumptions

This book assumes that you understand some basics of computing, such as the general idea of secure transactions and the need to know whom you are dealing with when working remotely. However, the book *doesn't* assume you know anything about eIDAS or earlier regulations involving security standards, nor anything about trust services, TSPs, or HSMs. We lay all that out in simple terms that anyone can understand.

# Icons Used in This Book

Throughout this book, in the margins, you'll notice some natty little eye-catching icons. But they're more than just page décor: They have a purpose, too. Here's what they signify:



REMEMBER

The paragraphs next to this icon spell out the most vital concepts contained in these pages. They identify the key information to file away in your brain, even if you remember nothing else!



TECHNICAL  
STUFF

This icon points out information that you have no pressing need to know, but may find interesting anyway. If you choose to skip over it, it won't affect the knowledge you gain from this book.



TIP

This icon identifies time- or frustration-saving ideas to help you get your head around eIDAS or improve efficiency.



WARNING

We're not wishing to alarm you in any way, but sometimes you need to be wary of certain pitfalls in life. This icon highlights issues to be mindful of relating to eIDAS.

## Where to Go from Here

Just start reading! You can use our description of the chapters in this Introduction as a guide. If you already understand the eIDAS Regulation and want to skip straight to the solutions that nCipher Security provides, start with Chapter 5!

## IN THIS CHAPTER

- » Knowing what safeguards existed before eIDAS
- » Looking into the basics of eIDAS
- » Comparing the roles of trust and identity services
- » Understanding what's already been achieved and what's still to come

# Chapter 1

## What Is eIDAS?

If you do business online in the EU – or you work with businesses or government agencies that do – you might have heard some buzz about eIDAS (pronounced *ee-idass*).



REMEMBER

*Electronic Identification and Trust Services (eIDAS)* is a European Regulation that was adopted in 2014, and took effect in 2016. It's designed to create consistent regulations and standards across the EU for electronic identities and for trust services supporting authentication and signatures. eIDAS ensures that electronic transactions are secure, no matter where they take place.

In this chapter, you'll learn the basic facts about the eIDAS Regulation. You'll find out why this Regulation was conceived, how its makers aim to maximise interoperability through standardisation across the EU, and where things have reached in its implementation.

### WHAT'S IN A NAME?

A *Regulation* is similar to a law that applies across all Member States. A *Directive* prescribes results to be achieved, but each Member State must make its own law regarding the implementation.

# Stepping Back in Time: Before eIDAS

It's been common knowledge for decades now that electronic identification and trust services for authentication and signatures would eventually become ordinary, everyday technologies in the EU. It has just been a matter of figuring out – as individual nations and as a coalition of EU Member States – how to implement those technologies in ways that work for everyone.



TECHNICAL  
STUFF

eIDAS is actually not the first EU initiative to address trust services. The Electronic Signatures Directive (Dir.1999/93/EC) was passed in 1999, which required that electronic signatures be considered the equivalent of written signatures in all Member States.

This earlier Directive had a narrower scope and allowed each country to take its own approach to implementation, whereas the eIDAS Regulation enforces a common approach. Yes, each country had to accept digital signatures on documents, but they couldn't necessarily understand *each other's* signatures because they often had incompatible electronic signing systems.

In fact, according to the European Commission, the haphazard way that the Directive was implemented across Member States made it de facto impossible to conduct cross-border electronic transactions. Further, the wording of the Directive assumed technologies such as smart cards and USB fobs: In 1999 these were state-of-the-art but have largely been replaced today by more modern alternatives, like mobile devices and cloud services. Nor did the Directive recognise that identification and authentication services other than electronic signatures could benefit from harmonisation across Europe.

As a result, the EU has had an ongoing consistency problem with signatures. Things worked fairly well within individual countries, but when citizens or companies wanted to do business somewhere other than their home country, complications often arose. Generally, guidance was needed to ensure that all aspects of the infrastructure for secure electronic transactions could be implemented seamlessly across the EU.

## THE COMPLICATIONS OF INCONSISTENCY

Consider a fellow we'll call Max. Max lives in Austria, but while he was on a holiday in Finland a few years ago, he found a perfect little vacation cottage for sale. Max visited a bank in Finland and filled out the paperwork for a mortgage, and then headed back home to Austria, with the idea that he would finalise the transaction electronically later in the month. The trouble came when Max found out that the Finnish and Austrian government agencies and banking institutions used different methods of electronic identification and document signing. The Finnish bank was not able to authenticate Max's online identity or accept his digital signature remotely. As a result, Max and the Finnish bank had to shuffle papers back and forth via overnight mail, with Max having to visit a local banking office in Austria to find notary services to authenticate his signature. So much for the paperless world of the future, eh?

The sidebar 'The complications of inconsistency' gives an imaginary example of the kind of frustrations this situation caused. Thousands of similar situations occurred each day across the EU, where the existing systems worked fine – until a national border was crossed. With more than two dozen countries each with their own regulations, it's folly to think that each legislature will come up with compatible standards without some guidance. With every passing year, it became clear that an EU-wide Regulation was needed.

## Understanding eIDAS

eIDAS is an EU Regulation that establishes consistent standards for electronic identities, authentication, and signatures. However the Regulation is more than a law. It's a way of building business among 23 million small and medium enterprises (SMEs) throughout 28 EU Member States (shown in Figure 1-1), enabling cooperation and growth within a single, secure, digital market.



**FIGURE 1-1:** The Member States of the European Union.



**TECHNICAL  
STUFF**

The full name for eIDAS is: Regulation (EU) No.910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC. Whew! Is it a wonder we just call it eIDAS?

eIDAS sets high standards for providers of identity services and providers of trust services for authentication and signatures, which will push up the level of security available to businesses and organisations. The amount of step-up needed will vary among organisations, and also among Member States.



**REMEMBER**

In some Member States the existing regulations are not that different from those put forth in eIDAS, but in other Member States there will be a steep upward climb for the security of many businesses and government agencies as they integrate their practices with compliant eID and trust service infrastructures. When EU standardisation is fully implemented, all Member States will comply with the same high standards.

The European Parliament and the European Council published eIDAS on 23 July 2014, and Member States were given a deadline of 1 July 2017 to migrate from the 1999 Directive to the eIDAS Regulation. Certain aspects, such as mutual recognition of electronic IDs among Member States, had a slightly later deadline for compliance of September 2018.

## The eIDAS vision

What will the digital EU look like when eIDAS is fully implemented? Here are some expected benefits:

- » A citizen can use electronic signatures and other trust services across the EU.
- » National electronic IDs will be recognised equally in all Member States.
- » Citizens can use their electronic IDs and electronic signatures to transact business across Europe.
- » Electronic documents will be legally recognised in any EU Member State, regardless of the Member State in which it was written.
- » Document seals and time stamps issued in any EU Member State will be considered valid in any other Member State.



TIP

You can see how eIDAS can simplify everyday life by watching a short film, “Back to the efuture: eIDAS” online: <https://www.youtube.com/watch?v=szErHIwoDCU&feature=youtu.be>.

## Who and what are affected?

The eIDAS Regulation impacts all providers of trust services that protect transactions over the public network. The Regulation places specific requirements on their operation and their correct implementation through the use of audits. eIDAS also requires that all government and public services in the EU recognise standard signature formats and pan-European identities. The trust provided by eIDAS affects just about any organisation that carries out transactions over the public network, in particular transactions involving commercial or legal matters where it’s important to be certain of the participants’ digital identities and their activities.

These activities are collectively referred to as digital services supporting a single digital market. Examples include services associated with:

- »» Travel-related transactions such as car hire
- »» Tax and financial statements
- »» Pharmaceutical records
- »» Legal and insurance contracts
- »» Banking agreements, including investments and loans
- »» Business-to-business electronic invoicing
- »» New third-party payment services, which are opening up traditional banking
- »» Securing access to public websites

The eIDAS Regulation also applies to commercial services that require an EU identity, such as the so-called ‘know your customer’ services in banking. Any trust service associated with authentication and signatures falls under the eIDAS Regulation.



REMEMBER

The individual consumer of these services doesn’t have to worry about eIDAS compliance; the burden for compliance falls on the organisations that provide trust services to the public. So, to use our earlier example in the sidebar ‘The complications of inconsistency,’ Max doesn’t have to worry whether the banks he deals with in France or Finland are eIDAS compliant. Because the Regulation applies EU-wide, he can assume that they are. The banks, on the other hand, carry the responsibility of ensuring their systems are compliant, so it’s important that they work with an eIDAS-compliant trust service provider (TSP).

If you’re reading this book, we assume that you’re somehow involved in a business or organisation that has a responsibility to your customers or your user base to ensure eIDAS compliance. While this stuff might be interesting (well, we think it is!), consumers don’t need to think about it, other than to be aware that the eIDAS trust mark (which you can find out about in Chapter 2) indicates that the provider is “qualified” for trustworthiness, any more than someone driving a car needs to know the specifications for its engine.



## What the Regulation contains

In a complex Regulation that dictates not only the desired effect but also how to achieve it, it can be helpful to break things down into multiple levels.



REMEMBER

The eIDAS requirements are specified in four levels:

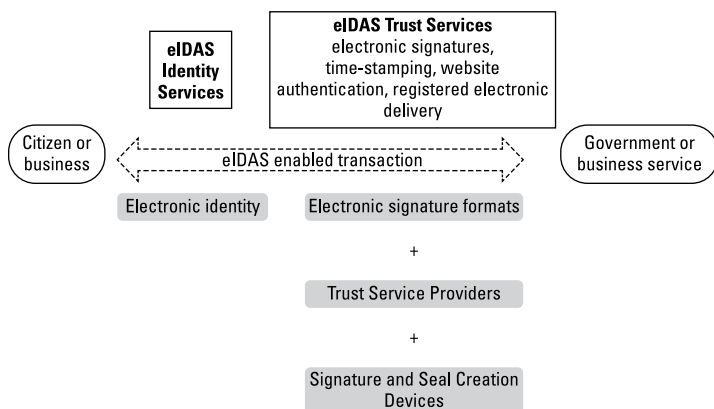
- » First is the regulation itself, which defines the basic requirements to be adopted across the entire EU. These requirements override any existing national regulations.
- » Second comes a set of standards that have been recommended by experts in the industry as a practical way of meeting the Regulation's requirements.
- » Third, accompanying the standards are EU implementing acts, which either mandate or recommend the use of the standards. To date, five implementing acts have been published, covering electronic identity interoperability and assurance levels, lists of qualified TSPs, signature formats, and signature and seal creation devices. You can find more information about these acts in the Appendix at the end of this book.
- » Finally, there are national rules that may extend or adapt non-mandatory standards to meet a nation's perspective. For example, some countries, such as Italy, accept registration via video link as being equivalent to face-to-face.

## Exploring the Role of Identity and Trust Services

The eIDAS Regulation has two key aspects: identity services, and trust services for authentication and signatures. These important services, also illustrated in Figure 1–2, may be defined as follows:

- » The first part covers eIDAS services for government-issued electronic identities – in other words, proving that a person or company is who they say they are, using an identity issued by the government. The Regulation doesn't require a single EU-wide identification scheme; however, it does require mutual recognition between national ID schemes.

» The second part covers eIDAS trust services for authentication and signatures. These are various activities that ensure mutual trust – in other words, confidence not only in all parties’ identities, but also that they are accountable for the actions taken. The trust services can include electronic signatures, time-stamping, website authentication, and registered electronic delivery.



**FIGURE 1-2:** eIDAS covers both identity services and trust services.

Take a quick look at each of those aspects individually in the following sections. We’ll get into much more detail in later chapters.

## eIDAS e-Identity (eID) services

*eID services* attempt to verify someone’s identity electronically. Depending on the transaction type, different levels of assurance of the person’s identity are appropriate, and eIDAS offers three progressively more certain levels: low, substantial, and high (these levels are described in more detail in Chapter 2).



REMEMBER

eIDAS does not provide for an EU-wide database of citizens; each Member State and organisation maintains its own databases. The eIDAS-mandated identity services component simply provides cross-border recognition on an as-requested basis. For example, when a citizen of a Member State presents her national eID to a government agency in another country, her home country’s database authenticates or denies the identification credentials.

## eIDAS trust services

As well as identity services, eIDAS provides guidance for trust services. These cover the following:

- » Trust services that support electronic signatures and its new variant, electronic seals
- » Trust services supporting website authentication
- » Trust services for registered e-delivery between authenticated parties



REMEMBER

eIDAS introduces a new legal concept called an *electronic seal*. An electronic signature created by an individual can be the legal equivalent of a handwritten signature. However, electronic signatures don't cover cases in which a document needs to be protected by a digital signature that represents an organisation rather than an individual. That's where electronic seals come into the picture. They use the same technology as electronic signatures, but are issued on behalf of an organisation rather than an individual, and don't have the same legal significance as signatures.

Under eIDAS a signature may be created using keys held on the user's device, or by keys *held in the cloud* by a trust service provider. *Signing in the cloud* is an alternative approach for electronically signing documents, whereby signing keys are held on a trust service provider's Hardware Security Module (HSM – check out the nearby sidebar for more information). This approach eliminates the need for users to handle their own keys. Cloud signing is growing in popularity and is having a significant impact on the market.

## The link between eIDAS eID and trust services

eID and trust services are covered by separate aspects of the Regulation with different approaches: eID extends government issued physical identity cards to the electronic domain, while trust services are aimed at trusted commercial services. However, they are closely related. Trust services often depend on the same identity verification checks required to issue an eID and commercial services that use public key techniques may be used for both eID and trust services. Moreover an eID may be used by a cloud-based signature service to remotely sign a document. This book is targeted mainly at trust services: however, many of the technical solutions described can be used both for eID and for trust services as defined by the eIDAS Regulation.

# HSMs: HARDWARE SECURITY MODULES

An HSM is a tamper-resistant device for creating high quality cryptographic keys and managing them securely. HSMs execute sensitive cryptographic operations that are secured by these keys. Chapters 3 and 4 dig deeper into the details of HSMs.



REMEMBER

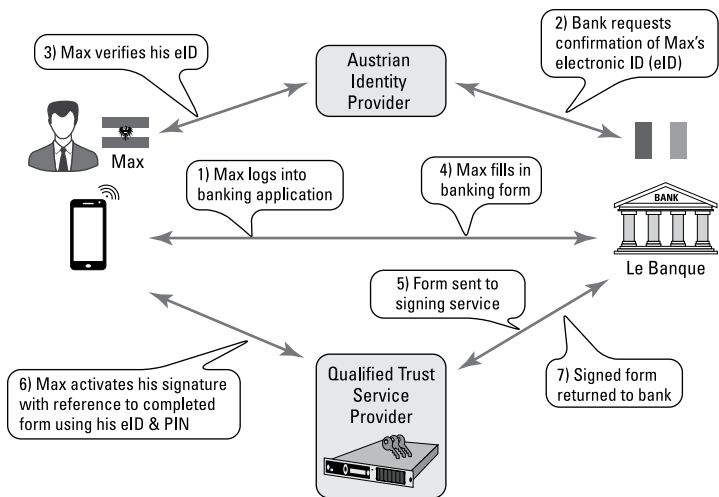
eIDAS regulates three elements of an electronic signature or seal. We'll look at these in more detail later, but here's a quick overview for now:

- » **The electronic signature format:** This defines the structure for encoding the cryptographic element of an electronic signature within a particular document structure, such as PDF, XML, or binary.
- » **The operation of a trust service provider (TSP):** The TSP provides security information: for example, a public key certificate supporting an electronic signature.
- » **The signature creation device:** This is a piece of hardware that generates the cryptographic element of an electronic signature. Older systems tended to use smart cards for this, but more modern systems typically rely on HSMs.

## How identity and trust services work together

The identity and trust services described in the previous two sections are easier to understand by looking at an example.

In Figure 1-3, Steps 1 through 3 illustrate the process using our Austrian friend, Max (from the earlier sidebar, 'The complications of inconsistency'), using a government-provided electronic identity (eID) to log into a banking application. That's identity services at work. Once logged in, he fills out a form (Step 4) and then signs it (Steps 5 and 6) and returns it to the bank (Step 7). Steps 4 to 7 represent the trust service's portion of the activity.



**FIGURE 1-3:** Identity and trust services working together.

## Figuring Out the Current State of Affairs

What's in place today? Well, for starters, there are lists of trust service providers and secure signing devices which are recognised as meeting the highest eIDAS quality requirements, referred to as Qualified. So, you may have a pretty good idea of the Qualified TSPs and devices that can be used to support the security of systems against known cyberattacks. Each TSP on the list has to be regularly audited against the eIDAS rules, which compares their practices to existing standards and industry-wide best practices, and a TSP can only remain on the list if the audit succeeds. We'll look at TSP qualification and auditing more closely in Chapter 2.

TSPs have been operating for many years, adhering to existing industry standards and best practices (which you'll learn more about in Chapter 2). For example, industry-wide standards for electronic signatures using older technology (such as smart cards) are in place. ETSI EN 319 411-1 and -2 already fully cover the standards for signing and website authentication, and audit requirements for TSPs providing time-stamping services are provided by ETSI EN 319 421.

The standards for the newer technologies are also available. A standard for HSMs (CEN EN 419 221-5), aimed specifically at eIDAS requirements, is formally agreed and has been extended

to support requirements for server-based signing (CEN EN 419 241). ETSI then used these CEN standards to specify trust service standards for signing in the cloud (called remote signing in ETSI TS 119 431 and TS 119 432). For more information see Chapter 3.

Further standards for signature validation using cloud-based trust services, registered e-Delivery (ETSI EN 319 521 & EN 319 522) and its adaptation to registered email (ETSI EN 319 531 and EN 319 532) have been published. A standard for preserving the integrity of signed documents for long after the signing keys have expired is nearing completion (ETSI TS 119 511 and TS 119 512).

Further standards are expected in the area of identity verification, which should be applicable to both eID and trust services. These will allow both face to face identity checking and remote identity checking using modern technologies such as video cameras and biometrics.



ANSSI, the French national agency for information systems, has certified the EN 419 221-5 Protection Profile for Hardware Security Modules. This standard is likely to replace FIPS 140 as being the required standard for EU governmental procurement of HSMs. The adoption of EN 419 221-5 is a step forward for customers, the market, and HSM manufacturers. It is enabling HSM manufacturers to certify their products as eIDAS compliant and will simplify the audit requirements on those trusted service providers who use an HSM certified to EN 419 221-5. nCipher Security were the editors for this Protection Profile in CEN, and were instrumental in its delivery.

## THE RELATIONSHIP BETWEEN ETSI AND CEN STANDARDS

The two main European Standards bodies, ETSI and CEN, have worked together to meet the requirements of the eIDAS Regulation. CEN provides standards for the security of signing devices and systems required by the Regulation such as HSMs and smart cards. ETSI defines standards for the trust services which build upon CEN-compliant secure devices. These cover requirements for the secure operation of trust services, such as their policies and practices, as well protocol standards which ensure interoperability between users and their TSPs, enabling users to easily switch between TSPs.



REMEMBER

It's important to remember that certification to a standard is just one way for TSPs to show compliance with the Regulation, which is the ultimate goal. If there is no eIDAS standard for a particular service, then the TSP must demonstrate compliance with its industry's best practices. The auditing process uses the best and most up-to-date standards available at the time, so auditing criteria may shift slightly as regulations are approved, particularly for new technologies such as signing in the cloud.



TIP

Because the eIDAS standards are still evolving, it's important that any trust service's system be made as future proof as possible, to avoid having to reauthenticate users and reissue keys. Because nCipher has been heavily involved with the standards, it can help customers create cloud signing systems building on existing solutions to use the recently ratified standards for signing in the cloud. Head straight on to Chapter 2 to find out more.

## IN THIS CHAPTER

- » Moving from paper to electronic IDs
- » Using trustworthy trust services
- » Looking at how TSP standards aid consistency
- » Figuring out auditing and qualification

# Chapter 2

## Electronic IDs and Trust Services

**M**ost people in the EU are accustomed to carrying a paper or plastic ID card with them wherever they go. But what if where they go is online? As technology has advanced, more and more activities that used to rely on in-person visits to stores, government offices, and financial institutions can now be handled online, so long as the participating parties can be confident of each other's identities. This chapter examines the past, present, and future of electronic IDs, and explains how they fit into the eIDAS Regulation.

Also in this chapter, we discuss trust services and TSPs, and the standards that govern them. *Trust service providers* (TSPs) are the companies that provide third-party trust services which support the user requirements for signatures and authentication. For example, they issue digital certificates and time stamps that businesses and government agencies rely on for assuring the integrity of their digital activities. You'll learn how TSPs achieve and retain qualification through audits.



# No Paper, Please! Electronic IDs

For any type of online communication, each party wants to be assured that the unseen person or business on the other end is who they say they are. The level of assurance required depends on the importance of the communication and the consequences involved in being mistaken or deceived.



WARNING

For sensitive matters, such as governmental activities like tax filing and voting ballots, a simple username and password might not be sufficient to prove identity. For these kinds of transactions, different measures have been employed in various EU Member States to validate someone's identity online by issuing an identity assertion that positively identifies a legal or natural person. Each Member State maintains the identity information for its citizens.

## Existing eIDs in Member States

Many EU Member States, including Belgium, Croatia, Estonia, Germany, Italy, Luxembourg, Spain, Portugal, and the UK, have adopted electronic ID (eID) systems. These ID systems typically consist of a chip-enabled plastic ID card that can be presented in person at a government office or read using some sort of card-reader or chip-reader hardware on a computer.

In the Estonian system, for example, a citizen can purchase a card reader that connects to her PC. When she wants to take part in an online transaction that requires identification, she inserts her card into the reader and inputs a PIN, much like when visiting an ATM. The Estonian government has a robust eID system that allows citizens to cast votes, file tax returns, refill prescriptions, access bank accounts, and more.



TECHNICAL  
STUFF

The problem up until eIDAS, as you can probably guess, is that each Member State was free to create its own digital identification system under the 1999 Directive. A project called *STORK* (*Secure idenTity acrOss boRders linKed*) has attempted to create identity standards across Europe, but lacking a legal foundation, its adoption has been limited. eIDAS technologies build on the technical features of existing cross-border electronic identity schemes such as STORK, adding to them as needed.

## eIDs under eIDAS

Under the eIDAS Regulation, a citizen's electronic ID must be recognised equally well in any Member State. This cross-recognition requirement applies to all government services, including health-care and tax registration, as well as to any business services that use official government-issued IDs to validate identities, such as banks, car-hire services, and airlines. Although eIDAS mandates mutual acceptance of eIDs only for public sector activities, not private sector ones, businesses that want to confirm a customer's identity (for instance to meet 'know you customer' requirements) can use government-issued electronic eIDs, both for their own convenience and to provide the highest level of customer service.

As mentioned in Chapter 1, the eIDAS Regulation is supplemented by multiple implementing acts. Requirements for interoperability between national schemes have been published in the 2015/1501 implementing act.



REMEMBER

eIDAS establishes three assurance levels for electronic identification: namely, low, substantial, and high:

- » **Low:** Uses simple authentication such as passwords with minimal checks on the identity when registering
- » **Substantial:** Using two-factor authentication: for example, with extra checks against a phone registered against the owner, with verification checks on identity when registering
- » **High:** Using sophisticated authentication mechanisms with comprehensive checks on an identity when registering



REMEMBER

There are three basic ways to authenticate someone's identity digitally. With two-factor authentication, identity providers verify the signer using any two of these ways:

- » Something that only the signer knows, such as a password or PIN
- » Something that only the signer has, such as a smart card or smart phone
- » Some unique, measurable physical characteristic of the signer, such as a fingerprint

Each Member State must accept eID schemes from other Member States that match the requirements of one of these levels. For example, Belgium and Estonia can mutually recognise each other's identity schemes. As a result, a citizen in Belgium could access an Estonian government service that requires high assurance identity verification, such as using her smart card to establish her citizenship ID. The requirements for each of these levels of assurance are detailed in the 2015/1502 implementing act.

eID mutual recognition across EU Member States became mandatory in September 2018. This later date was to help those Member States that had no experience with eIDs or that hadn't been involved in STORK. Member States that have *notified* eID schemes (schemes that are accepted by the EU) must now mutually recognise other notified schemes.

## Putting Your Trust in Trust Services

*Trust services* refers to a broad range of services for authentication and signatures for protecting electronic transactions.



REMEMBER

Trust services can include the following activities:

- » Issuing certificates for signing, sealing, and website identification, such as certificate authorities providing public key infrastructure (PKI) services
- » Issuing digitally signed time stamps
- » Long-term preservation of signed data: for example, ensuring the long-term validity of signatures on archived documents
- » Electronic registered delivery services, where evidence of delivery from an identified source is required
- » Signature and seal validation

The eIDAS Regulation came into force in July 2016, and by 1 July 2017, existing TSPs must have been audited against the Regulation. Until that time, they could continue to operate under the old Directive.

The nearby sidebar, 'Trust services: A quick example', shows just one example of how they may be used. Some specific industries require trust services in business-to-business transactions as well, such as the bio-pharmaceutical industry.

## TRUST SERVICES: A QUICK EXAMPLE

Here's an example of a trust service in operation that most people are familiar with. When a business creates a secure website that people can log into, they typically employ a digital certificate issued by a certificate authority to verify the authenticity of their website. This gives users confidence that their sensitive information, such as credit card numbers and account numbers, is not being snooped on or stolen. Most organisations don't single-handedly set up and maintain their own trust services. Instead, they employ the services of companies called *trust service providers* (TSPs). TSPs offer third-party services to help ensure the security of online transactions. A TSP is legally liable for any damage caused by its failure to comply with the Regulation's security measures, so it's expected that a TSP will employ and demonstrate best practices.

The European Telecommunications Standards Institute (ETSI) has established a set of standards for the basic services that TSPs are expected to provide, including public key certificates and time-stamping services. These standards are discussed later in the chapter. But first, here's an introduction to those essential services.

### Certificates and public keys

One way to ensure the identity of someone you are interacting with online is to have a third party vouch for them. You've probably asked a friend to provide a reference for someone who claims they know them, right?

*Hey Max, this guy over here says you two are old friends. Is that true?*

That's the basic idea behind public key certificates.



REMEMBER

A *public key* is a code string that uniquely identifies a certain individual or company. However the word *public* in public key doesn't mean the general public. In *public key cryptography* (also called *asymmetric cryptography*), keys come in pairs: a public key and a private key. The private key must be kept absolutely secure and not shared, whereas the public key can be shared with anyone.

Here are two scenarios involving Alice and Bob (who are famous in cryptographic circles). Bob wants to send Alice a message, and Alice needs to be sure that the message came from Bob. So Bob uses his private key to encrypt the message. Alice can then validate that the message came from Bob by decrypting it using Bob's public key. In the second scenario, Alice wants to send Bob a message that only he can read, so she encrypts it with Bob's public key. Then the only person who can decrypt it is Bob, using his very well-protected private key.

*Certificates* provide a way for a user to give her public key to someone, allowing the recipient to verify that the public key is genuine. A trusted third party (such as a TSP) creates a *digital certificate* (also known as a *public key certificate*) that validates the identity of the public key owner. The authenticity of a digital certificate is backed by the reputation of the TSP issuing it. A TSP issuing certificates is known as a *certificate authority* (CA).



TIP

A company or individual who wants the trust of customers or constituents online can contract with a TSP to issue a certificate on their behalf. Then when a secure transaction is initiated, the software checks the validity of the certificate, and if everything checks out the transaction continues. Otherwise an error appears.



REMEMBER

One of the most important functions as a TSP is to serve as a trusted CA. To make sure that the entire EU is operating using the same set of standards for certificate trustworthiness, the eIDAS Regulation specifies the basic requirements that any public TSP operating within the EU must meet.

## Time-stamping

The eIDAS *time-stamping* trust service provides proof of the existence of a document, its signature, or other information at a given time. This is achieved by binding together a digest (or *hash*) of the document or other information, with the current time using a signature from the trust service provider, as specified in IETF RFC 3161.



REMEMBER

Time-stamping has an important role in ensuring that documents that are stored or archived can be validated many years after they were signed. This can be used with the document's signature to prove that the signature existed at the time it was time-stamped. Thus, even if the circumstances around the creation of

the digital signature change (such as the signing key being later compromised and the signature being revoked), the signature itself remains valid.

Even if the document isn't signed, time-stamping can be used when archiving a document to protect its authenticity, proving its existence at a given time and ensuring that any changes can be detected.

Other methods are widely used to establish evidence of the time of signing, such as email and audit logs, but time-stamping is considered to be the most secure approach. Time-stamping provides proof of a signature's date and time, in a similar way that electronic identification provides proof of the signatory's identity.



REMEMBER

The date and time of an electronic signature can be legally significant in some situations. For example, suppose a client's electronic signature was verified by a certificate from a TSP, and then that certificate is discovered to have been revoked. The signature turns out to have been faked, and a huge lawsuit hinges on the question, "Who is responsible?" It all depends on when the signature was created.

Time-stamping isn't just for use at the time of signing – it's also for later, for the archival records of a company. You never know when a signature and its time stamp are going to become critically relevant. To support validation over the long term, the revocation information and CA certificates that were initially used to validate the signature need to be available indefinitely. Optional features of electronic signature and seal standards provide the capability to store this information along with the signature, as well as adding further time stamps on archived documents using state of the art cryptography.

The standards for time-stamping under eIDAS were published at the same time as standards for public key certificates. You learn more about them in Chapter 3.

## Links between eID and Trust Services

The eIDAS Regulation treats eIDs and trust services as having independent requirements. It views eIDs as equivalent to government-issued identity cards, whereas trust services are

commercially run services with governmental oversight. However, it's becoming clear that there are overlaps between the two. Under the Regulation a certificate issued by a trust service can be based on an identity proven using an eID, and more generally, eIDs can be used as part of the identity checks required by trust services. Moreover, cloud-based remote signing can use a government eID or a commercially issued identity token.

## Keeping Everyone Consistent: TSP Standards

As we noted in Chapter 1, nearly all the standards required to support eIDAS compliance are finalised, though they're being updated to take into account practical experience. New technologies such as blockchain are also being considered.

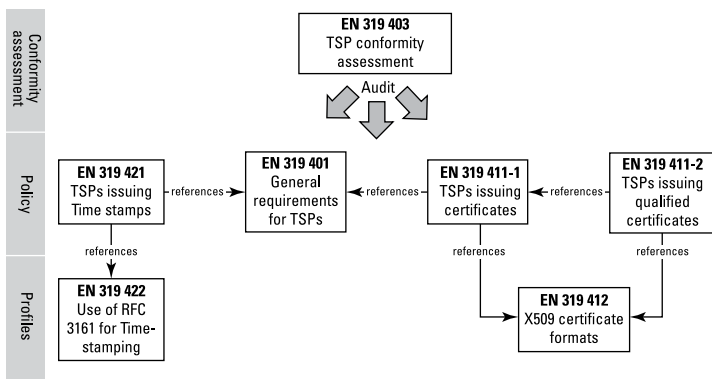


REMEMBER

The European Telecommunications Standards Institute (ETSI) has established a set of standards for public key certification and time-stamping services. Compliance with these standards is not mandated under eIDAS, but the supervisory bodies of many EU countries generally recommend them and they are the only recognised best practices for TSPs under eIDAS.

These ETSI standards ensure that the functionality of a trust service is aligned with industry best practices, and that the TSP's information security management system follows the generally accepted principles defined by ISO 27002. These standards align with – and build upon – internationally recognised profiles and standards for PKI services, such as those adopted by the CA/Browser Forum, the banking industry, and the SAFE BioPharma Association. Taken together, they represent a good basis for auditors examining TSPs with an eye toward best practice for eIDAS compliance.

The following sections provide an overview of these ETSI standards governing TSPs and their operation. As you review them, refer to Figure 2-1 to see how they fit together.



**FIGURE 2-1:** ETSI standards for public key certification and time-stamping services.

## ETSI general standards

What do all TSPs have in common, regardless of type? There are two general ETSI standards, governing the overall process:

- » **EN 319 403:** This standard provides detailed requirements for organisations that assess or audit TSPs to ensure legal compliance. Depending on the types of services they provide, TSPs will be audited against one or more of the more specific standards, as shown in Figure 2-1.
- » **EN 319 401:** This standard outlines the general policy requirements for managing and operating TSPs. The TSP can be a certificate issuer, time-stamp issuer, signature verifier, or an entity that uses electronic signatures or seals.

## ETSI standards for specific TSP types

Some standards apply only to certain types of TSPs and services, so they are addressed in specific sets of ETSI policies:

- » **EN 319 411-1:** This specification defines the policy and security requirements that are common to TSPs issuing certificates, also known as certificate authorities (CAs). It references EN 319 401 for generic requirements and EN 319 412 for certificate format requirements. The standard replaces TS 102 042 and is aligned with the CA/Browser Forum requirements.



- » **EN 319 411-2:** This standard defines the policy and security requirements specifically for qualified TSPs issuing qualified certificates in the EU, as specified in the eIDAS Regulation. For a discussion on qualified TSPs, see later in this chapter. EN 319 411-2 references EN 319 411-1 for the majority of the requirements and replaces TS 101 456.
- » **EN 319 412:** This standard profiles the use of X.509 certificate formats for individuals, legal entities, website certificates, and qualified certificates.
- » **EN 319 421:** This standard covers the policy and security requirements relating to operating and managing TSPs that issue time stamps. Such time stamps can be used in support of electronic signatures or for any application that needs to prove a document existed before a particular time.
- » **EN 319 422:** This standard covers the use of RFC 3161 data formats for time-stamping.

A series of standards have been published for registered electronic delivery and its specific use in registered electronic mail. The general policy and security for registered electronic delivery are defined in ETSI EN 319 521 with technical protocols and evidence formats defined in a multi-part standard, ETSI EN 319 522. ETSI EN 319 531 (policy and security) and ETSI EN 319 532 (technical protocols) specify how EN 319 521 and EN 319 522 are applied to registered electronic mail.

Specifications for the preservation of signatures and signed documents are expected to be published towards the end of 2019. This includes TS 119 511, which specifies policy and security requirements, and TS 199 512, which specifies protocols. These standards may also be applicable to preserving the integrity of any archived documents.



TIP

For more information about standards, see the Appendix at the end of this book.

## Knowing Whom to Trust: Qualification and Auditing



WARNING

Would you trust a salesman just because he claims to be trustworthy? Of course not! And neither should customers trust a TSP without some independent verification.

eIDAS introduces the concept of *qualification* for TSPs and cryptographic hardware. Under eIDAS, each Member State is responsible for maintaining its own list of qualified TSPs, and for determining the criteria for being on that list.



The criteria might differ slightly between Member States, but there are some basic must-haves and the criteria are much more similar than they're different. Each Member State must also specify criteria for the periodic auditing of TSPs to make sure they continue to comply with all requirements. These lists are made publicly available to other Member States and also to potential customers who are shopping for TSP services.

## Qualified TSP status

To be designated as qualified by a Member State, trust services must meet specific requirements defined by that Member State.

Qualified status is also applied to:

- » Certificates, which must be issued by a qualified TSP
- » Time stamps, which must be issued by a qualified TSP
- » Cryptographic hardware, which is can be used for signature or seal creation: for example, a QSCD
- » Electronic signatures and seals, which require a qualified signing device and a qualified certificate

The ETSI standards for TSPs (discussed earlier in this chapter) generally place the same requirements on TSPs irrespective of whether they are qualified or not. Specific requirements are included in the standards where it is necessary to add to generally accepted best practice with requirements specific to EU Qualified TSPs and their Qualified Certificates. The most important feature of qualified certificates is they're subject to direct regulatory oversight.



Qualified trust service providers are identifiable by a trust mark, as shown in Figure 2-2.



**FIGURE 2-2:** EU trust mark for qualified TSPs.

A *qualified signature creation device* (QSCD) is cryptographic hardware, such as a hardware security module (HSM), that has passed the certification process under the eIDAS Regulation.

Certified products are appearing following the publication of CEN EN 419 221-5 for certified HSMs and CEN EN 419 241-2 for the use of certified HSMs in remote signing.



TIP

If a signing device or TSP isn't qualified, that doesn't necessarily mean that you should consider it less trustworthy. Other schemes besides the eIDAS Regulation aim to ensure trustworthiness. For example, the CA/Browser Forum provides a similar international TSP approval scheme that is accepted by all the major application providers, in spite of being 'non-qualified' in relation to the eIDAS Regulation. However, especially for TSPs with customers in EU Member States, being qualified is a significant selling point for current and potential customers.



REMEMBER

Previously, banking was treated as a closed community, and hence not covered by eIDAS. However, the second Payment Services Directive (PSD2) opens up payment services to third party 'payment service providers'.

To support this open environment, eIDAS Qualified Certificates are used to secure communications between TPPs and banks.

Bank-to-customer services, such as establishing identity when opening an account, are regulated by PSD2.

## TSP auditing

So, how do TSPs get and keep that coveted spot on the qualified list? They submit their systems for *auditing*, in which an independent third party examines its physical, operational, and technical security. TSPs must be re-audited periodically to keep their status current.



TECHNICAL  
STUFF

How often must auditing occur? Article 20.1 of the eIDAS Regulation requires that qualified TSPs be audited every two years. Auditing is also a mandatory part of the CA/Browser Forum baseline requirements, which calls for an annual audit.

The eIDAS Qualified level is similar to the CA/Browser Forum's Extended Validation designation. ETSI has therefore established a set of standards for auditing TSPs that meets both the

requirements of the eIDAS Regulation and those of the CA/Browser Forum. As a result, a TSP needs to be audited only once to be approved under both standards. The TSP auditor will release two statements: one to the CA/Browser Forum pertaining to its extended validation, and one to the eIDAS regulatory authority pertaining to its Qualified status.



TECHNICAL  
STUFF

The CA/Browser Forum agreement has been adopted by the major web software providers, including Apple, Google, Microsoft, Mozilla, Opera, and Qihoo 360 (which serves over a third of the population of China), as well as most of the TSPs inside and outside Europe.

## Trust us! National lists of qualified TSPs

Each EU Member State is responsible for publishing a list of TSPs that its national supervisory scheme has recognised as Qualified, either under the eIDAS Regulation or the earlier Directive. A standard structure for this trusted list has been defined (TS 119 612) and is applied to eIDAS by Implementing Act 2015/1505. This standard structure includes an entry for each trust service, together with the TSP's certificate.



TIP

So if each Member State has its own list, how does that make for harmonization across the EU? Easy! The EU publishes one official list that complies links to every Member State's list. You can find that list at [https://ec.europa.eu/information\\_society/policy/esignature/trusted-list](https://ec.europa.eu/information_society/policy/esignature/trusted-list).

To say that these lists are large, complex, and ever-changing is an understatement. As of this writing, there are currently 1,400 entries distributed across 31 national lists, and changes can potentially occur every three days. Because of this, you can imagine the difficulties for application providers in incorporating the trusted lists into their applications. Adobe currently supports trusted lists, as do several providers of custom solutions for government agencies, but it is not yet clear whether other major providers will follow suit.



TIP

Trusted lists can also be checked on a case-by-case basis using the official EU list. The recommended tool for browsing the compiled list is available at the following URL:

<https://webgate.ec.europa.eu/tl-browser/#/>.

- » Finding out more about electronic signatures
- » Understanding the different levels of electronic signature
- » Looking into essential seal and signature standards
- » Checking out the old and new ways of signing

## Chapter 3

# Electronic Signatures: Click on the Dotted Line

When someone ‘signs on the dotted line’ on an important document that has legal force, it’s typical for one or both parties involved to ask for some third-party verification that the signature is genuine. You’ve probably been through the drill before with a paper document, right? First you drive to a bank, wait for the notary, show your ID, sign the document, and wait for the notary to affix a seal and signature. There goes an hour of your life that you’ll never get back.



REMEMBER

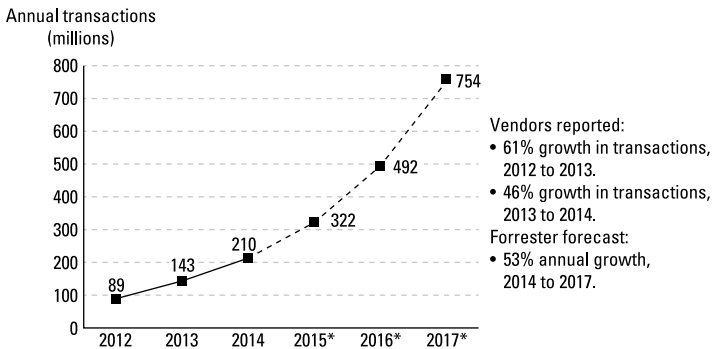
Signing documents electronically has been slow to catch on because of the security and verification difficulties involved. When you don’t physically see the person sign the document, how do you know it was signed on the date indicated, and by the person presenting the ID? Until recently, there haven’t been many affordable and trustworthy ways to make these transactions happen. This situation has changed in recent years, however, with the introduction of technologies that enable people to verify their identities and signatures with a high degree of certainty, and without spending a fortune to set up the system. Newer methods even allow individuals to use their own smart phones to sign devices, with the help of HSMs running behind the scenes.

In this chapter, we'll survey the landscape of electronic signatures, and you'll learn how they are addressed in the eIDAS Regulation.



Remember the Electronic Signatures Directive of 1999, which we told you about in Chapter 1? This EU Directive required that electronic signatures be considered the equivalent of written signatures in all Member States. Its original authors thought that this Directive was going to create a surge in electronic signature usage across the EU, but that didn't happen. One reason was the lack of cross-State compatibility (which eIDAS takes care of), but another was that the world wasn't ready for it yet. People were still entrenched in the idea that paper signatures were better or more reliable.

In the last several years, though, there has been rapid growth in adoption of electronic signatures. As shown in Figure 3-1, the analyst firm Forrester forecast that in 2017, over 700 million transactions would use electronic signatures. Forrester interviewed nine leading electronic signature solution providers, who reported combined annual growth of 53% since 2012.



Source: Forrester interviews with nine leading e-signature solution providers  
\*Forrester projection

**FIGURE 3-1:** Adoption of electronic signatures.

## Discovering Uses for Electronic Signatures

It's easy enough to say what an ink signature on a paper document is good for, right? It signifies the signer's agreement with the document, whether that document is a financial document

like a mortgage loan or an estate-planning document like a Power of Attorney agreement. Signatures don't have to be as formal as all that, though; you might sign a credit card charge receipt at a restaurant, or sign a business letter, without giving it much thought.



WARNING

A signature is only as good as the confidence you have that the person who signed is the actual person. For low-importance signatures, the signer's identity doesn't matter too much. For example, when a delivery driver comes to your door with a package, he usually doesn't care if you're the package recipient or not when he asks you to sign his clipboard. But for documents that trigger the transfer of financial assets, identity verification is imperative. That's why some important documents require a notary seal, to signify that a responsible party checked the signer's ID.

With an electronic signature, you don't, of course, have a trustworthy human comparing the picture on the signer's ID to their physical features, so there has to be another way of verifying the signer's identity.

The purpose of an electronic signature is to provide assurance that a document hasn't been modified after it's been signed and that it comes from an identified person. This is where electronic signatures are actually better (that is, more tamper-proof) than ink-on-paper signatures. A trust service provider (TSP) certifies that the public key used to create the signature belongs to the identified individual (see Chapter 2): The signature created using the certified public key authenticates the signer and ensures that changes to a document are detectable.

## Exploring Electronic Signatures

Just as differing levels of physical signature verification are appropriate in different situations, there are also different digital signature levels. The eIDAS Regulation defines two types of electronic signatures: advanced electronic signatures and qualified electronic signatures.



REMEMBER

Both advanced and qualified signatures are based on digital signature technology; however, an advanced electronic signature is less stringent than a qualified electronic signature. An advanced electronic signature, at the minimum, must be:

- » Uniquely linked to the signatory
- » Capable of identifying the signatory
- » Created in a way that ensures the signatory can maintain sole control
- » Linked to the data it relates to in such a manner that any subsequent change to the data is detectable

A qualified electronic signature must meet all the requirements for an advanced signature, and in addition must be supported by the following components:

- » A qualified signature creation device, such as a smart card or HSM, which is certified by Common Criteria and meets the requirements of the eIDAS Regulation. You can read more about Common Criteria in Chapter 4.
- » A qualified public key certificate issued by a qualified TSP, which has been audited by an accredited organisation and found to address the requirements of the eIDAS Regulation (see Chapter 2 for more information).

## DIGITAL SIGNATURE VERSUS ELECTRONIC SIGNATURE – WHAT’S THE DIFFERENCE?

An *electronic signature* can be any kind of online or computerised signature, including an email message or word processing document. It’s the generic idea, referring to the legal concept of signing something electronically.

A *digital signature* is a technical solution, involving public key certificates and cryptography, used to meet the legal requirements for the advanced and qualified electronic signatures just described.

However, don’t rely on all documentation to adhere to that distinction; the terms are often used interchangeably.





REMEMBER

A qualified electronic signature is assumed to have at least the legal equivalence of a handwritten signature. A judge must determine the veracity of any other type of electronic signature.

## Gaining the (Electronic) Seal of Approval

Sometimes it's more appropriate for a company or organisation to approve a document, rather than an individual. For example, when a nonprofit organisation publishes its by-laws, those by-laws are a product of the entire board of directors, with no one particular person as the author.



REMEMBER

The eIDAS Regulation introduces the concept of an *electronic seal* that can be used in situations where individual signatures aren't suitable. An electronic seal is similar to an electronic signature, in that it uses the same technology. Like electronic signatures, electronic seals can be either advanced or qualified. However, an electronic seal has a different legal meaning, in the following ways:

- » The source of an electronic seal is generally assumed to be a legal entity or organisation, whereas an electronic signature comes from an individual.
- » Seal creation is under the control of one or more individuals authorised to represent the organisation. (Recall that with individual electronic signatures, being under individual control was a defining hallmark of the technology.)
- » Seals don't provide the same legal indication of intent by an individual, but they do provide assurances as to the authenticity of information provided by the business.

Whereas an electronic signature is specifically for legal signatures, an electronic seal is concerned with authenticity and integrity. Sealing has quickly become important for business-to-business exchanges, such as order processing and invoicing, and business-to-consumer exchanges, such as issuing receipts. Recently, the European banking industry adopted the use of electronic seals, supported by Qualified Certificates, to secure open-banking transaction for the new third-party payment services that interact with banks on behalf of banking customers.



TIP

Electronic seals have proved to be a useful tool. Although electronic seals are a new legal concept in many EU countries, they are becoming increasingly popular for securing business transactions.

## Understanding Essential Seal and Signature Standards

The eIDAS implementing decisions make no technical distinction in the standards between electronic signatures and seals. The same signing device (such as an HSM or smart card) can be used to create either a signature or a seal. With that in mind, here are some specifics for digital signature and seal standards.

CEN have published advice (in CEN TR 419 210) on how its standards can be used for evaluating devices as Qualified Electronic Seal Creation Devices under the eIDAS Regulation.

Qualified Electronic Seals that meet the requirements of the Regulation can be created using such Qualified devices. Qualified Electronic Seals must also be created using digital signatures for instance, AdES signatures as described below and must be supported by a Qualified Certificate issued specifically for Qualified Electronic Seals.



REMEMBER

eIDAS Article 27 (and implementing decision 2015/1506) requires that online government services recognise standard formats for advanced electronic signatures and seals. The collection of standards that govern these formats are known as AdES (which, as you might surmise, is an acronym for advanced electronic signatures).

AdES is based on existing ETSI standards, but includes two additional features to ensure an electronic signature or electronic seal can be validated long after a document was signed:

- » The signing certificate must be included in the calculation of a digital signature's cryptographic value.
- » Optional time stamps can be added to the signature to assist in long-term validation.

AdES covers the use of these standard digital signature formats for electronic signatures or electronic seals:

- » **CAAdES (EN 319 122): Cryptographic Message Syntax (CMS) Advanced Electronic Signature/Seal:** This standard is based on a binary structure, and is applicable to any data format.
- » **XAdES (EN 319 132): XML Advanced Electronic Signature/Seal:** XAdES digital signatures are most appropriate to XML data.
- » **PAAdES (EN 319 142): Portable Document Format (PDF) Advanced Electronic Signature/Seal:** Only for PDF documents, this standard covers details of how signatures should be presented and displayed, and integrated into a form submission process. The result is that PDF editing and rendering tools inherently support digital signing, whereas the use of CAAdES and XAdES will generally require separate tools for editing and signing.
- » **ASiC (EN 319 162): Associated Signature Containers:** This standard covers the application of signatures to a package of files, such as a ZIP folder.

There are plans to introduce JAdES, another AdES format, to protect JSON formatted signatures. JSON is a data syntax specifically for use with Javascript, so JAdES will enable electronic signatures and seals to be used in a web environment. JAdES will be based on JSON Web Signatures as defined by RFC 7515, with additional features that may be needed to support the Regulation (for example, protection against certificate substitution and long term validity).

In addition to these, ETSI EN 319 172 defines general rules for creating and validating any AdES format. The AdES implementing decision 2015/1506 references earlier versions of the above standards; however, the differences are not significant and shouldn't inhibit interoperability.



WARNING

Businesses may use other formats. However, when government services are involved, or other regulations are in place to mandate the use of advanced electronic signatures, the approved AdES formats are required.

## Smart Card Signing: The Old Way

Authenticating users for electronic document signing has always been a challenge, ever since the 1999 Directive went into effect. How do you ensure that someone is really who they say they are, and that they're authorised to sign a particular document?

Prior to the eIDAS Regulation, digital signature systems have mostly been administered using smart cards. A user would present a smart card to a signing service provider, and the smart card would provide both proof of identity and signing functionality. For example, a bank employee might present a smart card to provide proof of identity, and use it to generate a signature for a document that the employee presents to a tax collection agency.

Smart cards have their drawbacks, though. Keeping a smart card safe and secure can be difficult – and keeping thousands of them safe and secure can be an administrative nightmare. Issuing smart cards to everyone in an organisation who needs to securely sign documents can be expensive and administratively unwieldy, particularly for organizations that may have to support millions of users. People frequently lose or misplace smart cards, so a large organisation may need extra employees to reissue cards and re-authenticate users who request replacements. Another concern is that smart cards often have to be reissued as new security standards emerge. As a result, the adoption rate for smart cards for electronic signing has been low in the EU.

## Signing in the Cloud: The New Way

Rather than trying to protect signing keys in all those smart cards, what if a TSP protected all the signing keys in a single, easy-to-administer location, and then allowed users to connect to it remotely? That's the basic idea behind *signing in the cloud*, a new feature introduced by the eIDAS Regulation.



REMEMBER

The eIDAS Regulation uses the term *remote electronic signatures* when referring to signing in the cloud. However the CEN EN 419 241-1 and -2 standards (which we discuss later in this chapter) refer to *remote signing* or *remote signatures*, and Adobe talks about *cloud signatures*.

With signing in the cloud, TSPs use HSMs to hold keys on behalf of their users, rather than storing keys on smart cards.

Users work with a cloud signing service that employs a certified HSM, such as an nCipher *nShield* product. The HSM securely holds the keys, so there is no risk of it being lost or stolen. Users can safely enter their credentials and sign documents using a smart phone, tablet, computer, or other electronic device that has web-browsing capability.

HSMs support remote signing services by executing these tasks:

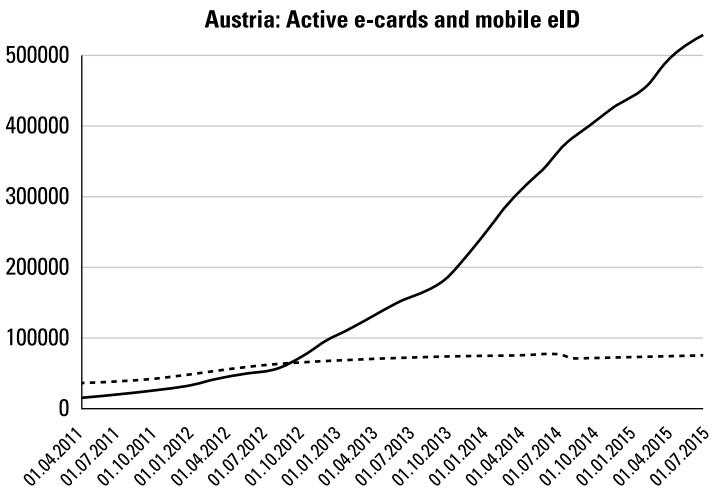
- » Securely authenticating the signer (the user)
- » Creating and protecting a signing key for each user
- » Ensuring that a document can only be signed with an authenticated user's signing key



REMEMBER

The details of an HSM's cryptography may be complex, but the process from a user's standpoint is pretty simple. A user creates an electronic signature through a cloud-based service online. The user's signing key is held within an HSM operated by a TSP, which she can activate through a mobile device.

How big is signing in the cloud? *Huge*. Moving forward, the predominant approach for electronic signing will be through HSMs and mobile devices. For example, in Austria, mobile device usage more than tripled in a four-year period, as shown in Figure 3-2, while the use of smart cards has stagnated. This dramatic market shift is also happening in other countries across Europe.



Source: Presentation on the Austrian mobile ID at the European Telecommunications Standards (ETSI) Security Week, Sophia-Antipolis, June 2015 ([www.etsi.org/news-events/events/870-security-week](http://www.etsi.org/news-events/events/870-security-week)).

**FIGURE 3-2:** Use of mobile devices (solid line) compared to smart cards (dotted line).

## Four elements for trustworthy cloud signing



REMEMBER

A practical cloud signing implementation depends on four elements:

- » **The HSM (the signing device) that holds the user's signing key:** The HSM must comply with recognised standards, and must be stored in a secure location.
- » **Signature activation:** This is the process of authenticating and activating the user's signing key. It is important that the user's key is under her sole control at all time: The security of cloud signing depends on it. Signature activation is achieved through a secure exchange between the user's personal device and the HSM holding her signing key. This exchange between signer and HSM is mediated by the Server Signing Application.
- » **The security of the user's personal device to be used for signing, such as her smart phone:** The personal device must be protected against malicious software, and access to the device must be protected, such as by a password, PIN, or fingerprint.



WARNING

If a smart phone is used to hold an authentication key or biometric information, some trust element may be necessary. However, it may not be possible to mandate that every user have a secure smart phone, so some compromises may be required.

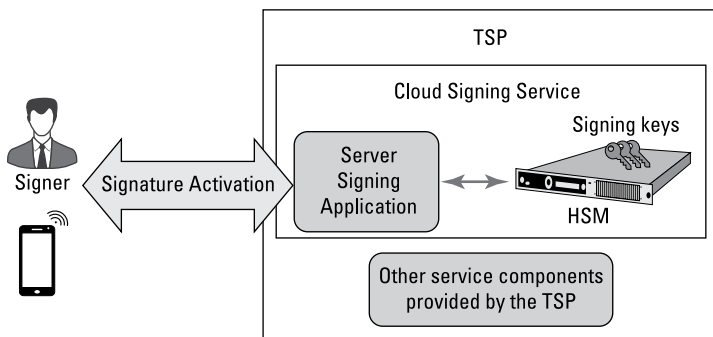
- » **The TSP that operates the cloud signing service, probably as part of a wider TSP service:** Regular audits ensure the TSP's trustworthiness. These audits look at the security of the entire system, including physical and operational measures, and the TSP's ability to meet the functional requirements expected of the cloud signing service.

Three of these elements are regulated by two eIDAS requirements:

- » Requirements for certified QSCDs cover the HSM (the signing device) and activation of the user's signing key.
- » Requirements for TSP audit cover the TSP that operates the cloud-signing service.

The security of the user's personal device isn't directly addressed in eIDAS, but will be driven by the terms and conditions the TSP imposes on its users. These terms and conditions are reviewed as part of the TSP's audit.

Figure 3-3 illustrates a potential approach to remote signing using an HSM.



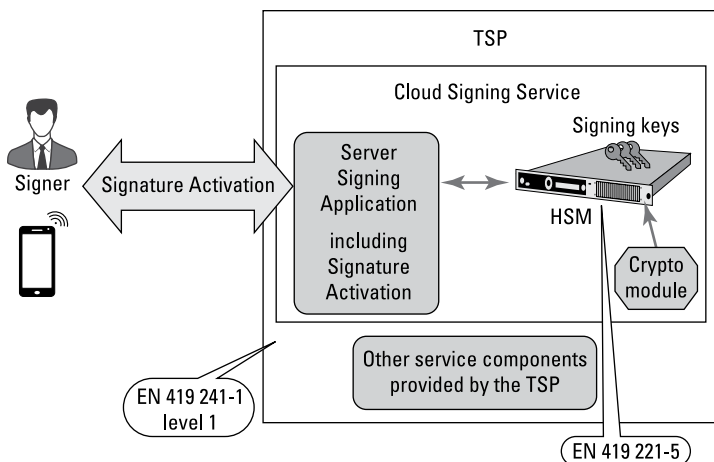
**FIGURE 3-3:** Signing in the cloud.

## Cloud signing standards

A set of CEN standards for devices, and a set of ETSI standards for trust services, have been defined for signing in the cloud. The CEN standards (EN 419 241-1 and -2) cover the requirements for the signing device. EN 419 241-1 defines the general requirements for operating the signing device for remote signing, while EN 419 241-2 defines the specific security requirements of the signing device that follows the general eIDAS standard for HSMs, EN 419 221-5.

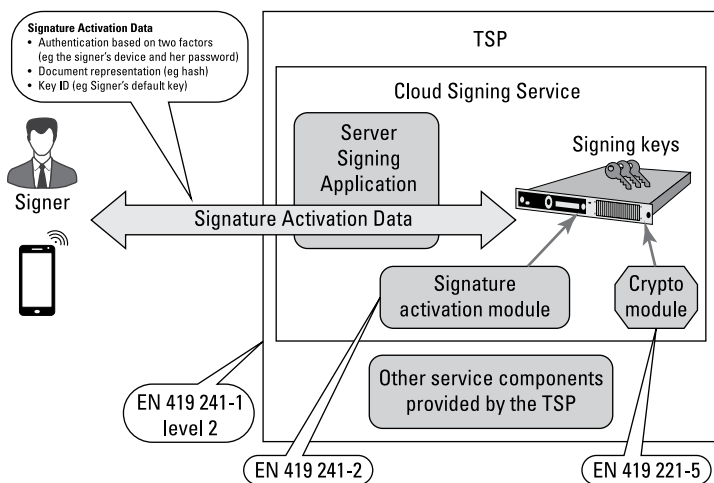
EN 419 241-1 identifies two levels of sole control assurance, level 1 and Level 2:

- » Level 1, illustrated in Figure 3-4, relies on the server signing application to ensure that the appropriate signing key is selected. The functionality supporting signature activation and ensuring sole control is implemented as part of the server signing application. This level can use any suitably certified HSM, such as one certified to EN 419 221-5.



**FIGURE 3-4:** Cloud signing, Level 1.

» Level 2, illustrated in Figure 3-5, provides greater assurance of sole control by requiring code within the HSM to implement signature activation. This code is certified to the same security level as the HSM's general cryptographic functions. The signature activation data passes, in protected form, from the signer's device to the HSM to ensure that the user's signing keys can't be abused, even if the TSP's server signing application were to be compromised.



**FIGURE 3-5:** Cloud signing, Level 2.



For Level 2, although not explicitly stated, the Common Criteria Protection Profile EN 419 241-2 is expected to be necessary. This requires that the code evaluated under EN 419 241-2 operates within a general purpose HSM conforming to EN 419 221-5.

ETSI has built on the CEN standards, providing a set of standards for trust service security, policy requirements, and protocols for signing in the cloud. ETSI TS 119 431-1 defines the security and policy requirements for operating a CEN EN 419 241-1 conformant device to ensure that it is secure and meets the requirements of the CEN standard. ETSI TS 119 431-2 defines for requirements for TSPs provisioning digital signatures that conform to the AdES formats as described earlier.

The Cloud Signature Consortium (<https://cloudsignatureconsortium.org/>) is a group of industry and academic organisations with interests in cloud signing. The Consortium have defined a web service API to provide a standard interface to CEN and ETSI based cloud signing services. The API can be used by a signing application, perhaps running on a mobile phone. Functions provided include retrieving information on a signing service and requesting a signing service to sign a document with a key held by the service. The API creates the required Signature Activation Data to ensure that the signing key is authorised by the user.



WARNING

As with many of the specifics of eIDAS, the legal requirement for cloud signing is still somewhat, dare we say it, cloudy. The eIDAS implementing decision for qualified signature and seal creation devices (EU 2016/650) calls for security that is comparable with a certified smart card device until the commission recognises specific standards for cloud signing. For the moment, many countries are opting for a level 1 approach, although interim solutions at level 2 based on the earlier TS standard are accepted by some countries. Once there is a recognised Common Criteria Protection Profile, such as prEN 419 241-2, the implementing decision will likely change to reference this standard.



TIP

Yes, there's a lot of uncertainty at the moment, particularly until the CEN standards we've discussed are adopted by the EU regulators, but this isn't stopping signing in the cloud from being widely adopted in the EU. nCipher Security's partners are already delivering cloud signing solutions within the eIDAS framework. By using the *nShield* architecture, these partners can provide customers with a clear migration path to standards-based solutions that are recognised throughout the EU.

# Use of HSMs for Electronic Signatures and Seals

The eIDAS standard for HSMs, CEN EN 419 221-5, was originally intended for TSPs operating in a secure and audited environment. When applying the CEN HSM standard to user environments, measures need to be taken to ensure the secure operation of the HSM, for example in a protected data centre. CEN has recently published a standard, CEN TS 419 221-6 *Conditions for use of EN 419 221-5 as a qualified electronic signature or seal creation device*, which proposes additional measures that users of EN 419 221-5 conformant HSMs must take in order to ensure secure signing and sealing under the Regulation. However, EN 419 221-6 is not yet recognised under the Regulation.

- » Investigating why you need an HSM
- » Knowing what to look for in an HSM
- » Sorting out the standards
- » Selecting your HSM supplier

# Chapter 4

## HSMs in the eIDAS World

The eIDAS Regulation brings benefits that should make everyone happier, like having a reliable and consistent set of standards to adhere to which make it more straightforward to deliver services that can be deployed throughout the EU, and like having a trust mark that means the consumer can be assured of the TSP's trustworthiness.



REMEMBER

HSMs have for some time been an important part of PKI and other trust infrastructures, and in particular they provide the root of trust by protecting the TSP's cryptographic keys. Because of this important role, eIDAS includes requirements that assure the HSM's trustworthiness.

Under the eIDAS Regulation, several kinds of trusted services require HSMs in order for the TSP to become qualified. We'll look at these scenarios in this chapter.

An HSM is a major purchase, so choosing the right HSM will pay off many times over. All HSMs are not alike – not by a long shot. There are important features to consider when shopping for an HSM solution, such as certification, flexibility, and future-proofing, and in this chapter you'll learn how to identify the right HSM for your TSP needs.

# Recognising Why You Might Need an HSM

Whenever you're holding cryptographic keys for trust services, it is essential that the keys are protected against misuse. The best way to achieve this is by using specialised security hardware – that is, an HSM.



TIP

Even if you're already using an HSM, under eIDAS you may find new opportunities that can benefit from their use. For one thing, HSMs are a lot easier to manage than smart cards, and can save thousands of Euros annually in administration costs compared to older-technology alternatives. But generally, there are three scenarios under eIDAS that require the TSP to use an HSM:

- » Signing certificates and time stamps, as well as other trust services.
- » Document signing in the cloud.
- » Document sealing.

Take a look at each in turn.

## Signing certificates and time stamps

Certificates and time stamps issued by a TSP must be signed using an HSM. Along those same lines, revocation information, such as provided via Online Certificate Status Protocol (OCSP) services and Certificate Revocation Lists (CRLs), must also be signed using an HSM. Some other TSP services, such as those for electronic registered delivery, signature validation, or long-term signature preservation, will also have objects that need to be signed, and so will require the use of an HSM.

## Document signing in the cloud

To enable documents to be signed in the cloud, the eIDAS Regulation allows a user's signing key to be held centrally by a qualified TSP on behalf of the user. However, to be compliant the TSP will need to hold the signing key within an HSM. See Chapter 3 for further information on cloud signing and the requirement for HSMs.

## Document sealing

As we discussed in Chapter 3, the eIDAS Regulation recognises a particular form of signature that represents an organisation, called an electronic seal. The signing key for a seal is held in a cryptographic device, such as an HSM or smart card, that is under the control of the organisation through one or more authorised individuals; unlike a signing key, more than one person may control the use of a sealing key. Seals can be used to protect information produced by a trusted *process*, such as one initiated on a computer within the organisation's data centre, rather than a trusted *individual*.

## Knowing What to Look for in an HSM



WARNING

If your organisation needs an HSM, the last thing you want to do is rush out and buy the first one you find – or worse yet, the cheapest one you can find. As with anything, you get what you pay for.

This section lists some of the most important features to look for in an HSM.

### Check the certification

Companies functioning as TSPs don't have to worry much about the nitty-gritty details of how an HSM works. There are big-brain technical experts to figure that part out.



REMEMBER

The most important thing you should shop for in an HSM is assurance of regulatory compliance. Has the HSM you are considering been through the certification or qualification process? More importantly, did it pass?



TIP

With the eIDAS standards for HSMs yet to have formal EU approval, it's important to find an HSM that will not only be conformant today, but also in the future. That means you will want to go with an HSM from an industry-leading company with its finger on the pulse of the eIDAS regulatory process.

The nearby sidebar explains more about current European and U.S. certification standards. Directive 1999/93 didn't contain specific requirements for HSMs, but only requirements which were

aimed at smart cards that could be adapted for HSMS. Article 51 of eIDAS (Transitional Measures) allows signing devices certified under the Directive to be used under eIDAS. As a result, HSMS that were Directive 1999/93-conformant are also good-to-go for eIDAS.



TIP

A list of certified devices, including those recognised through transition measures, is published by the commission at: <http://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>.

## Search for scalability

An HSM solution should be able to change as the business's needs change, without having to scrap the whole thing and start over. The company should be able to easily add hardware and software capabilities with minimal interruption.

## CERTIFICATION STANDARDS IN EUROPE AND THE U.S.

European governments already have a general scheme for certifying security products in place called *Common Criteria*. Common Criteria has become widely accepted, not only by EU Member State governments, but also by European industries, international companies that want to sell in the EU, and non-EU governments that tend to follow the EU's direction, such as southern Mediterranean and South American companies. Both EU and non-EU governments are increasingly adopting Common Criteria.

HSM certification for eIDAS is based on Common Criteria.

The U.S. Government has its own security-related regulations, such as the Federal Information Processing Standards (FIPS). FIPS is the *de facto* standard in the U.S., but is not accepted by a number of governments, including France and Germany, and some South American countries. Also, delays in delivering updates to the FIPS HSM standard and mistrust in FIPS has encouraged the uptake of Common Criteria.

But don't worry: nCipher *nShield* HSMS have both FIPS and Common Criteria certification, so they can meet regulatory requirements the world over.



TIP

A trust service might have to manage tens of thousands of keys, or even more. Look for an HSM solution that provides scalable key management and offers capabilities for key creation, loading, and backup.

## Bend toward flexibility

An HSM is an expensive investment, so the ability to support a range of TSP services under eIDAS with the one HSM helps to ensure a return on that investment. It should be possible to use the same HSM for the services described previously (for certificate signing, time-stamping, document signing in the cloud, and document sealing) as well as to meet other security needs of the business such as data privacy.



REMEMBER

Flexibility also means the ability to extend the use of an HSM to support additional functions: for instance, user authentication. As we explained earlier, the trend is toward using mobile devices rather than smart cards for authentication. However, it's important that users can authenticate through any device they choose, whether that's a laptop, tablet, smart phone, or authentication token. Organisations should also give users the flexibility to go through any channel they prefer, whether it's EMV/CAP, VASCO, RSA, OATH, SAML assertion, or digital certificate.



TIP

A number of nCipher partners have products based on nCipher HSMs, with support for the necessary authentication between the user, the service, and the HSM, for signing in the cloud.

## Establish what can be protected

As well as meeting the requirements for the specific services listed earlier, an HSM must satisfy the generic TSP security requirements to protect its own or its customers' sensitive information. For instance, an HSM ought to be able to protect databases and web and application servers.

Your HSM must also integrate readily with the applications you run, like Microsoft Certificate Services PKI or Entrust Authority Security Manager. And take a look for Java application server support, domain system security extension (DNSSE) integration, and code signing.

## Find out about running apps securely

TSPs can enhance the security of important or sensitive applications by running them within the HSM, using a secure execution environment. By doing so, they protect their custom applications against insider and Trojan attacks. A secure execution environment enables sensitive security software to be loaded and executed within the HSM's security boundary.



TIP



WARNING

The nCipher *nShield* HSMs provide a secure execution environment called *CodeSafe*.

Why might you want to run an application within the HSM? Think about this: A user's authentication credentials, to be secure, should be transmitted through a secure tunnel to the HSM, ensuring that they are never accessed by the service itself. The entire security of remote signing depends on the tamper-proof verifiability of the remote signer's identity. If the application that authenticates the user is run outside of the secure boundary, how are you going to be sure that it's not being faked? Running the authentication application within the HSM provides that assurance. In particular, services for document signing in the cloud will need a secure execution environment to run the sensitive functions required by the eIDAS Regulation.

## Sorting Out the Standards: Three Examples

We throw a lot of different standards and specs at you in this book, so perhaps now is a good time to look at a few examples of the standards specifically aimed at HSMs.

### Signing certificates and time stamps

Currently, France and Germany mandate Common Criteria-certified HSMs that are recognised under their national rules for signing certificates and time-stamping. For the rest of Europe, the use of Common Criteria certified HSMs is recommended for TSPs, though FIPS certified HSMs are accepted.





WARNING

Once the Common Criteria-based standards for HSMs are recognised under the eIDAS Regulation, the same standards will be applied across Europe, and FIPS will no longer be acceptable.

The HSM doesn't have to be specifically recognised as a qualified signature or seal creation device (as defined by the eIDAS Regulation); however, it is best to follow the generally recognised standard for HSMs under eIDAS: EN 419 221-5.

## Document signing in the cloud

Here's an area where things aren't quite solid yet. Regulatory requirements have yet to be agreed across the EU, although some nations have established national requirements. However, there are some basic expectations.

Now that CEN EN 419 241 (parts 1 and 2) are approved, new systems are expected to follow these standards. Here's what is required:

- » An overall server signing system that conforms to EN 419 241-1, with conformance verified by an audit
- » An HSM that has been certified under Common Criteria to EN 419 221-5
- » A secure execution environment within the HSM (such as CodeSafe) to run the specific code, certified under Common Criteria to EN 419 241-2, as required for remote signing

However, given the investment on signing systems that were not evaluated under Common Criteria, alternative evaluation schemes such as that provided by A-SIT may provide an acceptable alternative to CEN EN 419 241-2.

## Document sealing

Most of what's required for document sealing is the same as explained earlier in 'Signing certificates and time stamps.'

The only currently recognised certification for sealing is EN 419 211, which is a Common Criteria protection profile based on smart cards. In time, the intention is that EN 419 221-5 will be recognized for sealing.



TIP

Whatever your scenario, using an HSM that is certified to EN 419 221-5 will make it much easier to achieve compliance with the Regulation.

## Choosing Your HSM Provider

Throughout this book, we focus pretty heavily on the various standards involved in the eIDAS Regulation. In practice, of course, a user will experience the services, not the hardware or the regulations behind it.

Because of the eIDAS Regulation, government agencies and businesses that deliver online services can trust their TSPs to deliver critical security services that meet all required standards, so they can focus on delivering a high-quality experience to their users.



REMEMBER

The standards being adopted under eIDAS impose specific requirements on HSMs, and also make having an HSM more useful and desirable, especially with new-concept security solutions like electronic seals and cloud signing.

Ultimately, if you go with a well-respected HSM provider like nCipher Security, you shouldn't have to worry about eIDAS compliance. nCipher *nShield* HSM products have the certifications required for use under eIDAS. These products provide the flexibility and scalability to enhance performance and secure the digital assets used in just about any government or business service, whether it's procurement management, health care, banking, national ID, or invoicing.



TIP

Ready for the next step? Check out the sidebar, 'nCipher HSMs tick all the boxes,' and take a look at Chapter 5 to learn more about nCipher products and services and see how they might fit into your organization.

## nCIPHER HSMs TICK ALL THE BOXES

Here's an easy time-saver when shopping for HSMs: We recommend starting with nCipher *nShield* products, because they have everything you're looking for.

nCipher *nShield* HSMs:

- Have been certified to the latest available standards for eIDAS qualification. If you go with an *nShield* product, you don't have to worry about whether your system is eIDAS-compliant.
- Provide scalable key management for any size of business and any volume of key services.
- Offer users the flexibility to authenticate with any device type, through any channel.
- Integrate easily with the applications you run.
- Include a secure execution environment called *CodeSafe* for running sensitive software. It enables HSM functionality to be extended to support applications such as cloud signing.
- Are suitable for operation in dark data centres and in cloud deployments.

## IN THIS CHAPTER

- » Finding out how nCipher Security can help your business
- » Becoming certified, versatile, and future-proofed

# Chapter 5

## Ten Ways nCipher Can Help You

In earlier chapters, we discussed what the eIDAS Regulation consists of, and how it will change the way businesses and governments exchange secure data electronically across the EU.



TIP

Are you ready to get down to the business of bringing your organisation into compliance? You'll need a trusted partner, not only to provide the needed hardware, but to offer professional advice and to help you plan for the uncertainties of the future. With this in mind, we'd like to introduce you to nCipher Security, and the *nShield* line of products.

## Benefitting from Advice and Consultancy from an Industry Leader

In this time of uncertainty over the eIDAS Regulation and its implementation, it's comforting to have an experienced and trusted partner on your side.



REMEMBER

nCipher Security has many years of experience securing the world's most sensitive information, and is the most trusted and widely recognised name in the industry. nCipher Security HSMS provide data protection for more than 10,000 customers across 100 countries, including:

- » 21 NATO member countries
- » 15 of the Fortune 30 companies
- » 19 of the world's 20 largest banks
- » 3,000 financial institutions worldwide
- » 4 out of 5 top energy companies
- » 4 out of 5 aerospace companies
- » 20 leading cloud service providers



TIP

nCipher Security's industry leadership attracts the brightest and best worldwide, and the company employs some of the most respected engineers and analysts in the field of digital data protection and cryptography. That means that when you work with nCipher, you get advice and thought leadership from the technology experts who are helping to define the eIDAS standards.

nCipher Security's Professional Services Group has many years' experience of supporting its customers in meeting EU regulatory requirements, and in meeting regulatory requirements in specific industries, such as banking. The Group is ready to assist you to ensure that your HSMS are correctly deployed and that your cryptographic applications are configured to conform to industry best practices.

## Ongoing Commitment to the eIDAS Standards

nCipher Security has been working closely with the EU technical organisations that are creating the specific requirements for eIDAS implementation. As security experts, the nCipher team knows what works well – and what doesn't. Throughout the process of transitioning from earlier standards to eIDAS, nCipher is right there in the thick of things, advocating to ensure that the final standards will meet the needs of the community. For

instance, nCipher has been closely involved with EN 419 221-5, which ensures that HSMs are eIDAS compliant, and EN 419 241-2 for signing in the cloud.



REMEMBER

This close relationship between nCipher Security and the standards-making organisations means that nCipher constantly reviews its products to make sure they are meeting current market demands. If something is going to change regarding eIDAS that may affect a customer's system, the nCipher team is on top of it. nCipher customers can be confident that as the eIDAS regulations evolve, so too will nCipher products.

## Using Certified HSMs

nCipher Security *nShield* Connect, Connect+, Solo, and Solo+ HSMs are eIDAS compliant through the eIDAS transitional measures, having been certified under Directive 1999/93.



TIP

You can check this out through the EU's published list of devices recognised as Qualified Signature and Seal creation devices at: <http://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>.

nCipher Security's new *nShield* XC HSMs will also be eIDAS compliant by being certified against the Common Criteria Protection Profile, EN 419 221-5.

## Getting Help with Qualified Signature and Seal Creation Devices

As described in Chapter 3, the eIDAS Regulation defines two types of electronic signatures: advanced and qualified. Qualified is the more stringent standard, and requires a qualified signature creation device (QSCD) certified by Common Criteria. Does your HSM qualify?

If you use nCipher *nShield*+ HSMs, the answer is yes. The entire range of *nShield*+ HSMs are certified under Common Criteria and formally recognised as QSCDs under Article 51 (Transitional Measures) of the eIDAS Regulation.

This means that nCipher Security certified HSMs can be used for:

- » Signing certificates and time stamps issued by a Trusted Service Provider under the Regulation.
- » Signing revocation information for Certificate Revocation Lists and for Online Certificate Status Protocol (OCSP) revocation.
- » Signing objects created by other trust service providers for such things as electronic delivery or long term electronic signature preservation.
- » Remote signing with an HSM, and key management. nCipher works closely with partners to deliver comprehensive signing solutions that use current *nShield* HSM products. When there are thousands of keys involved, signing in the cloud using smart cards becomes infeasible. However, nCipher HSMs can manage the large numbers of keys needed for practical cloud signing solutions.
- » Document sealing, for situations where a signing key is under the control of an organisation rather than an individual. As described in Chapter 3, a seal is like a signature except it represents an organisation (such as a company or department) rather than an individual.
- » Protecting information exchanged between the new third-party payment service providers and banks under the 2nd Payment Services Directive of 25 November 2015 (EU) 2015/2366.



TIP

The complete list of Qualified Signature Creation Devices currently approved under the Transitional Measures can be found at: <http://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds>.

## Using Signing Certificates, Time Stamps, and Other Objects

As covered in Chapters 3 and 4, nCipher *nShield* HSMs can be used by TSPs who are signing certificates, time stamps, and other objects. They can also be used for signing revocation information.

It is recommended, and in many cases required, that HSMs used for eIDAS trust services are certified through Common Criteria (see Chapter 4), which of course includes nCipher *nShield* HSMs.

## Discovering Multi-Use Versatility

You'll recall from Chapter 4 that flexibility and versatility are important attributes of an HSM. An nCipher *nShield* HSM can serve multiple purposes, including all the eIDAS services. For example, the same HSM can be used for local signing, signing in the cloud, sealing, and other TSP functions. It also supports other non-eIDAS security functions that require the use of HSMs, including PKIs, database security, DNSSEC, and GDPR.



REMEMBER

nCipher HSMs have the performance, capacity, and design to support large numbers of client applications, each of which may be delivering a different service.

## Implementing Practical, Compliant Solutions

As explained at the end of Chapter 4, nCipher *nShield* HSMs tick all the boxes on a company's wish list. Not only do they have the required certifications, but they also provide the functionality needed to deliver practical, compliant solutions. They can:

- » Be purchased in different form factors to meet any company's needs, from embedded appliances to networked devices.
- » Securely store customer information, providing peace-of-mind about data privacy.
- » Integrate with many third-party applications, including leading database systems.
- » Provide the performance needed for large-scale deployments.
- » Handle and manage large volumes of customer keys.
- » Be managed remotely.



# Future-Proofing Your Systems

nCipher *nShield* HSMs can be updated as needed to accommodate new technologies and standards as they develop.

What if you need to future-proof a system against any upcoming changes as the standards develop? Not a problem. Partners can use the *nShield* CodeSafe environment for customised security sensitive code. nCipher is working with partners to develop solutions and CodeSafe applications to meet future standards, such as the authentication and key activation functions required for compliance with EN 419 241-2, the eIDAS standard for signing documents in the cloud.

# Gaining Support for Cloud Deployments

nCipher *nShield* HSMs provide many features to help customers deploy their systems in the cloud. For instance, Remote Administration, Remote Configuration, and High Availability support allow most administration and configuration tasks to be carried out remotely (great for dark data centres) and for cryptographic applications to be run independently of which HSMs are online at a given moment.

Within the context of the eIDAS Regulation, the nCipher cloud signing solution delivers signing in the cloud.

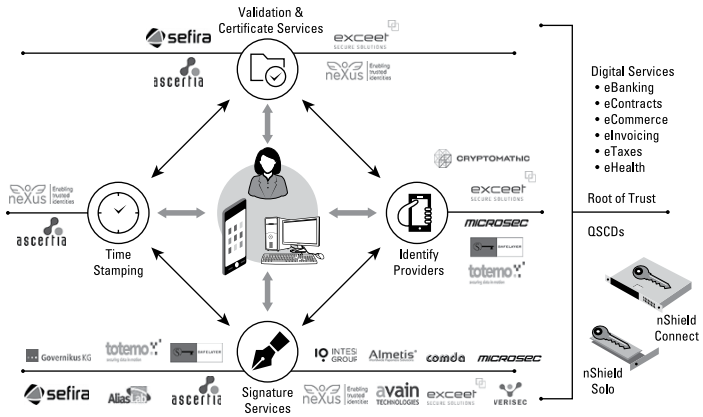
# Discovering a Powerful Ecosystem



REMEMBER

When you work with nCipher Security, you connect with a strong ecosystem of partners and suppliers. Whether you are looking at signature services, certificate and validation services, identity provisioning, or time-stamping, there is a partner you can work with.

Figure 5-1 shows some of the relationships that you can leverage as an nCipher Security customer. These include identity providers, signature services, validation and certificate services, and time-stamping.



**FIGURE 5-1:** nCipher Security proudly partners with industry experts to deliver comprehensive, compliant solutions.

- » Knowing what is scheduled to happen (and when)
- » Following a standards roadmap
- » Heading online to find out more

# Appendix

## Further Information

You're looking at this book's final few pages now, but maybe you need more specifics? Never fear, you've come to the right place! This appendix offers up some reference information you might find useful.



Feel free to consider this whole appendix as having a giant Technical Stuff icon stamped over each page! It contains the type of nitty-gritty detail that's useful to have on hand but is most helpfully presented in a fact-focussed end section rather than being scattered throughout the book.

## Checking the Timetable?

Implementing eIDAS, and developing all the supporting implementing acts and standards, is an ongoing process in the EU, which began in 2014 and will continue for the next few years.

Here are the key dates to be aware of:

- » **July 2014:** eIDAS Regulation came into force.
- » **September 2015:** Implementation acts took effect covering signature formats, electronic identity assurance levels, and electronic identity interoperability framework.
- » **July 2016:** The start date for the majority of technical requirements for eIDAS and for existing TSPs to migrate to

eIDAS audits. Newly regulated qualified trust services (such as time-stamping and signing in the cloud) must have been audited by this date.

The old 1999 EU Directive became invalidated, and all conflicting national rules were repealed and replaced. Any references to the 1999 Directive are to be treated as a reference to the eIDAS Regulation from this point on.

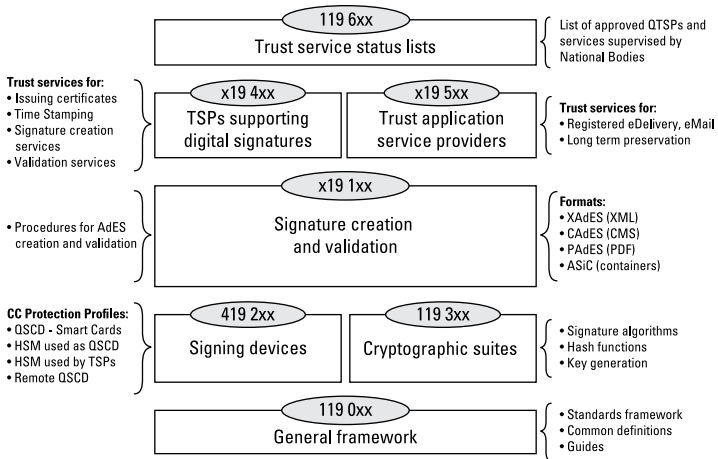
- » **July 2017:** A qualified TSP delivering a service that is currently regulated under the Directive must be audited by this date.
- » **May 2018:** CEN EN 419 221-5 was published.
- » **July 2018:** CEN EN 419 241-1 was published.
- » **March 2019:** CEN EN 419 241-2 was published.
- » **2020:** The Regulation will be reviewed.

## Mapping the Big Picture: A Standards Roadmap

A *standards roadmap* listing all the standards relating to trust services and signatures is described in the ETSI publication TR 119 000. These standards are grouped together by a numbering scheme, as shown in Figure A-1. This diagram may help you see how the many different standards fit together in a coherent whole.

Here are some references to the various standards involved:

- » **ETSI standards** can be obtained through the ETSI standards search page at the following URL: [www.etsi.org/standards-search](http://www.etsi.org/standards-search).
- » **CEN standards** can be obtained through any European national standards organisation.
- » **Specifications for eIDAS electronic identity services** are not issued through the formal standards bodies but are published through a European group comprised of national experts. These specifications may be downloaded at the following URL: <https://joinup.ec.europa.eu/software/cefeid/document/eidas-technical-specifications-v10>.



**FIGURE A-1:** Framework of eIDAS trust service related standards.

## Finding Out More Online

*Still hungry for more details? Here are some additional references to the related regulatory requirements:*

- » Trust services and electronic identity in the digital single market: <https://ec.europa.eu/digital-single-market/en/trust-services-and-eid>.
- » Regulation (EU) No 910/2014 (eIDAS): <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN>.
- » Implementing acts supporting eIDAS:
  - Commission Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (text with European Economic Area (EEA) relevance): [http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL\\_2015\\_235\\_R\\_0001](http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001).

- Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (text with EEA relevance):

[http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL\\_2015\\_235\\_R\\_0002](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002).

- Commission Implementing Decision (EU) 2015/1505 of 8 September 2015 laying down technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (text with EEA relevance):

[http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL\\_2015\\_235\\_R\\_0005](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0005).

- Commission Implementing Decision (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (text with EEA relevance):

[http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL\\_2015\\_235\\_R\\_0006](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0006).

- Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market:

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D0650&from=EN>.

## About the Authors

**Jonathan Allin** is a product manager for nCipher Security. He is an expert in European and global regulations, and is responsible for the certification strategy of nCipher's nShield Hardware Security Modules. He regularly speaks on the societal impact of identity and trust.

**Nick Pope** is Director of his own company, Security & Standards Associates, providing advice on the use of IT security standards. He has been involved in standardisation supporting eIDAS and the earlier EU eSignature Directive since 1999, and is currently Vice Chair of the European Telecommunications Standards Institute Technical Committee for Electronic Signatures and Infrastructures (ETSI TC ESI), responsible for standardisation for trust services under eIDAS.

## Are you ready for eIDAS?

The European Union's Electronic Identification and Trust Services (eIDAS) Regulation has created a single European market for secure electronic commerce. That's big news for businesses and consumers alike, because it means citizens of every Member State will be able to securely identify themselves and sign documents online, from the comfort of their homes or the on-the-go convenience of their mobile devices.

If your organisation offers secure digital ID and document signing services, you may need to make some changes in the way you handle these transactions to comply with the new regulation. Not sure what your organisation is facing, and how to proceed? This book can help.

### Inside...

- Why eIDAS was created, and how it helps the EU
- What's finalised about eIDAS, and what's still in flux
- How trust service providers (TSPs) become "trusted"
- What electronic document signing and sealing can do
- How remote signing with mobile devices is replacing smart cards




Go to **Dummies.com**<sup>®</sup>  
for videos, step-by-step photos,  
how-to articles, or to shop!

ISBN: 978-1-119-65222-9

Not For Resale

for  
**dummies**<sup>®</sup>  
A Wiley Brand

 Also available  
as an e-book





# **WILEY END USER LICENSE AGREEMENT**

Go to [www.wiley.com/go/eula](http://www.wiley.com/go/eula) to access Wiley's ebook EULA.