eIDAS2: What Prospects and Stakes for Digital Trust?

Pierre-Jean VERRANDO – General director
Alban FERAUD – President
C&ESAR 2022 - November 15th 2022

Executive summary

1. **About Eurosmart : a strong track record in cybersecurity & digital identity**

2. **eIDAS 2 file**
   - Overview
   - Digital identity
   - Trust services

3. **eIDAS 2 file : Cybersecurity aspects**

4. **Conclusion**

Executive summary

1. **About Eurosmart : a strong track record in cybersecurity & digital identity**

2. **eIDAS 2 file**
   - Overview
   - Digital identity
   - Trust services

3. **eIDAS 2 file : Cybersecurity aspects**

4. **Conclusion**

About Eurosmart
Who we are

Key facts

- The pioneer association dealing with digital security topics in Europe
- The initiator of two SOG-IS MRA technical groups: ISCI-WG1 and JHAS
- A community of recognised experts in the field of security evaluation, digital ID, including biometrics and blockchain
- Strong involvement in European digital identity files since 1999 (directive on electronic signature), and active contributor to eIDAS 1 (2014)

Advocacy and technical groups

- Cybersecurity and Digital Identity
- Biometrics
- Internet of Things
- Artificial Intelligence
- Maintenance of SOG-IS ISCI WG1 & JHAS: instrumental for CC evaluation at highest level on secure hardware
- Supporting document for security certification: ITSC
- Market & Technology

About Eurosmart
Who we are – the cornerstone of cybersecurity ecosystem in Europe

Companies

CYSEC, PayCert, XILINX, INTERNET OF TRUST, WISeKey, THALES, FINGERPRINTS, winbond, Tiempo SECURE, SARAPIS, Qualcomm, PROVE & RUN, Infineon, SAMSUNG, IDEMIA, IN GROUPE, NXP, TRUSTED OBJECTS, augmented

Testing, inspection & certification and laboratories

TRUSTCB, SGS, jtsec, KEOLABS, brightsight, RED ALERT LABS, SERMA, leti

Associations & research organisations

SPAC, Fraunhofer, ISEN

About Eurosmart
Eurosmart's 2022 topics

Certification and standards	Identity	IoT
EU CC Scheme	eIDAS / EUid	Cyber resilience Act
EU Scheme maintenance	Mobile driving licence	Security & conformity certification
EU standardization strategy	Digital Travel Credential	RED

Data protection and privacy

Emerging technologies, Post quantum cryptography, blockchain, AI…

About Eurosmart
Main activities in cybersecurity and digital identity in 2022

Digital identity/eIDAS 2 file

- ITRE hearing in eIDAS file (European Parliament)
- Hearing at eIDAS expert group
- Hearing at EU CoR
- Meetings and numerous written contributions to MEPs, DG CONNECT, PR….

Cybersecurity & market access

- Cyber Resilience Act (CRA)
- Radio Equipment directive

CE

Support high security certification

- Support security certification of secure hardware up to AVA_VAN.5
- PP 0117 Secure Subsystem on Chip
- Methodology for easy certification of hardware product making use of SoftIP


Certification Report

BSI-CC-PP-0117-2022

for

Secure Sub-System in System-on-Chip (3S in SoC) Protection Profile, Version 1.0

developed by

EUROSMART

EUROSMART'S PP-0117 RECEIVES A CERTIFICATION AWARD BY THE GERMAN FEDERAL CYBERSECURITY AUTHORITY (BSI)

Executive summary

1. **About Eurosmart : a strong track record in cybersecurity & digital identity**

2. **eIDAS 2 file**
   - Overview
   - Digital identity
   - Trust services

3. **eIDAS 2 file : Cybersecurity aspects**

4. **Conclusion**

eIDAS 2 file : Overview
Purposes

Digital identity : draw lessons from eIDAS 1 (2014) especially the shortcomings

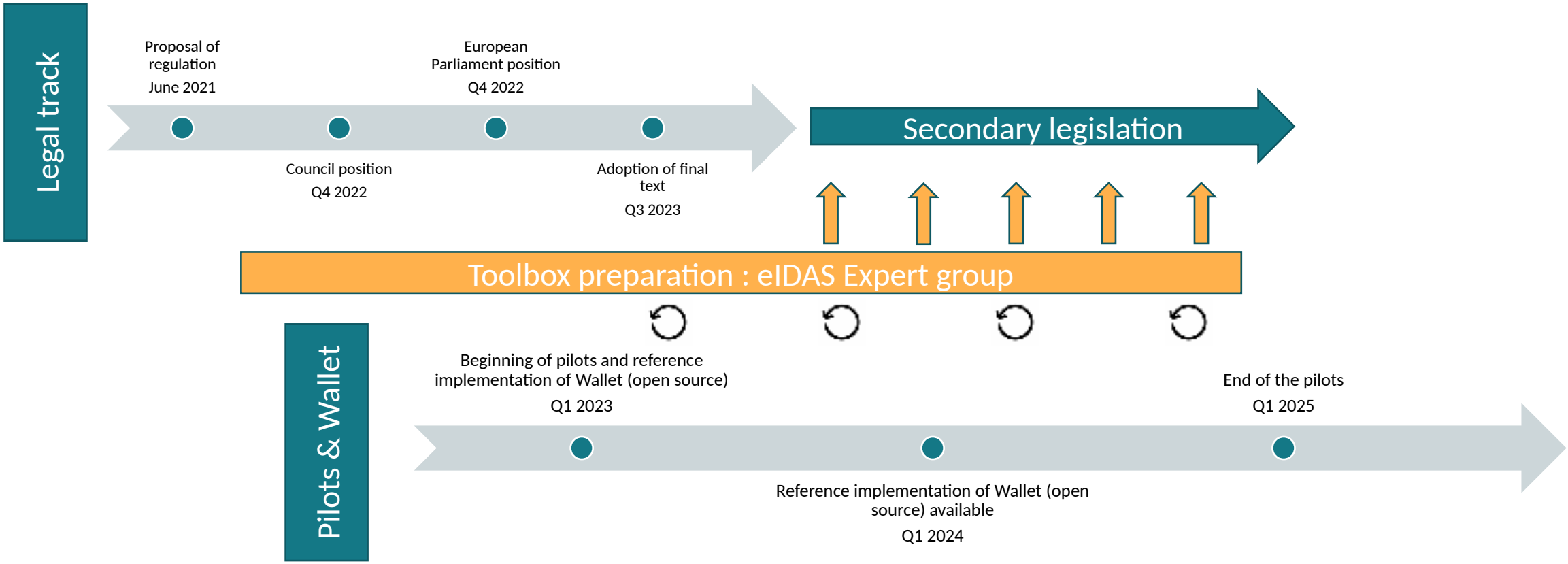
- Identification of individuals : remove ambiguity
- Scope of application: usage of digital identity with private sector
- Interoperability : direct interaction between the relying party and the user
- Management of attributes other than legal identity
- No mandatory issuance of digital identity

"***By offering a European Digital Identity framework based on the revision of the current one, at least 80% of citizens should be able to use a digital ID solution to access key public services by 2030.***"

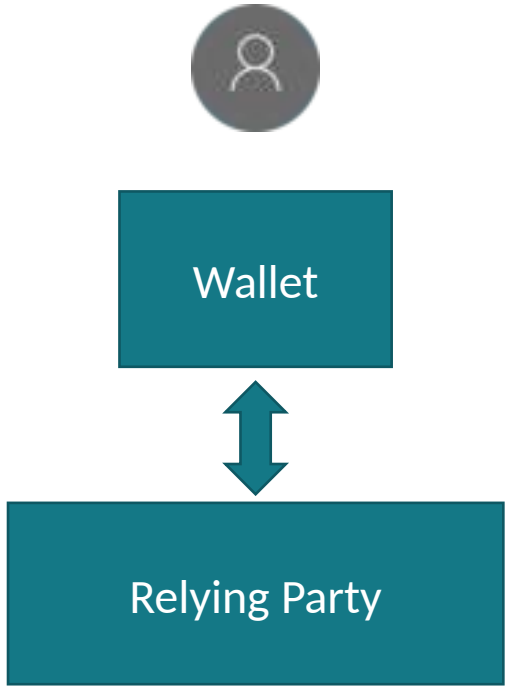
Trust services : update to (1) support the new digital identity framework, (2) increase security and trust, and (3) introduce new qualified trust services

Trust services may be used for various usages, not necessarily linked to digital identity

eIDAS 2 file : Overview Planning



eIDAS 2 file : Digital identity Approach



Wallet : user centric approach

Privacy

- Store data
- Allow selective disclosure of data
- Ensure sole holder control

Features

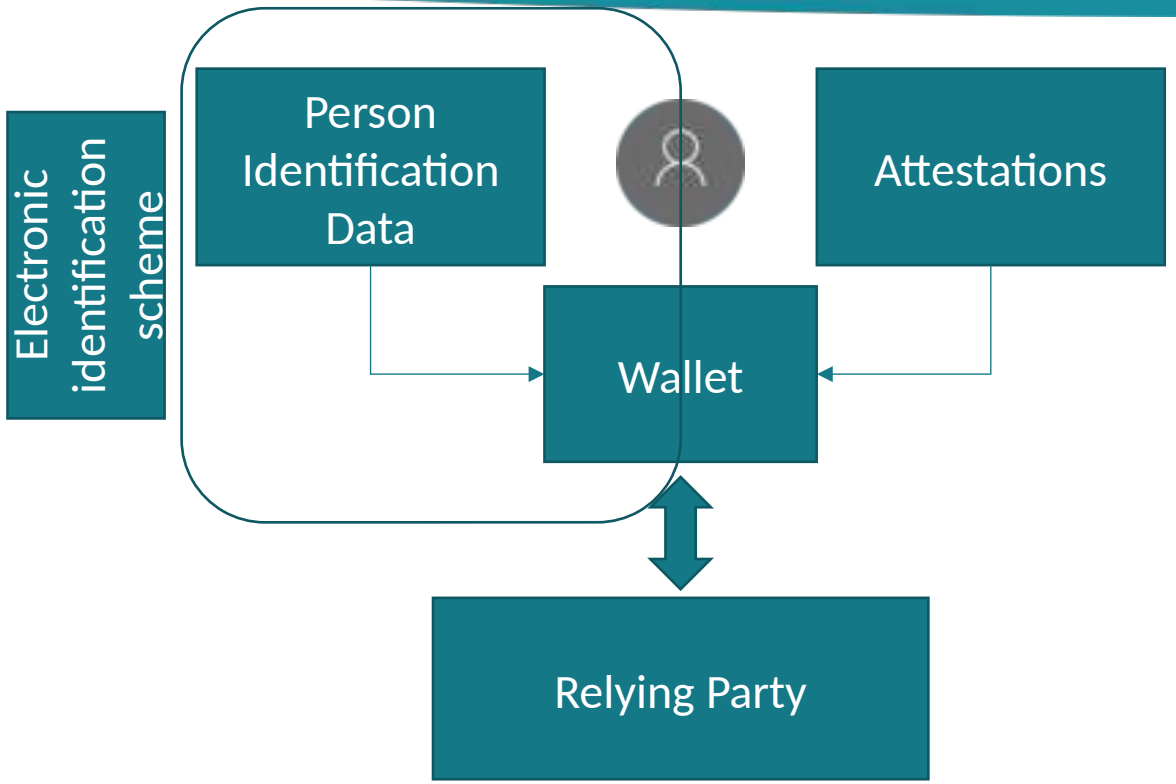
- Allow creating qualified signature (and/or seal)
- Electronic identification
- Allow presentation of data

Usable for online and offline transaction (except for qualified signature/seal)

Interoperability at wallet edge

=>The text introduces its own definition of wallet

eIDAS 2 file : Digital identity
Two types of data



Two types of data

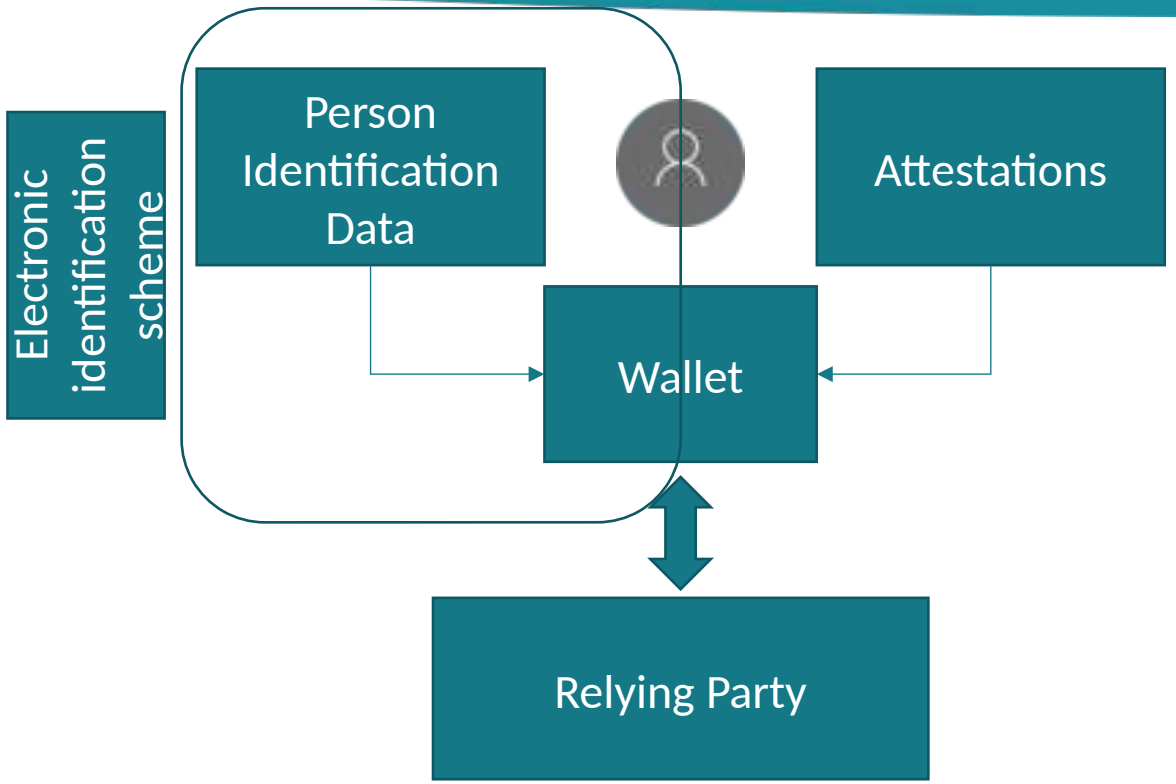
Person Identification data

- ~Legal identity - Unambiguous identification of holder
- Stored within the wallet, which shall be an electronic identification means of level of Assurance “High”
  - Authentication in the course of a transaction
  - Bound to its holder
  - High level of security
- Be issued under an electronic identification scheme

Attestations (of attribute)

- Attribute that are attested by an issuer
- Attribute are of any kind (age, address, driving license,…)
- Not directly relates to identity
- Many issuers (bank, phone operators,….)

eIDAS 2 file : Digital identity
Key measures for a large uptake



Large availability of wallet

Mandatory issuance & reference implementation of wallet (open source)

Foster trust

Wallet shall be highly secure, guarantee data protection, and be an electronic identity means of level of Assurance “High”

Large acceptance

Mandatory acceptance of the wallet for some types of Relying parties
Easy interaction with the wallet (mandatory standards at wallet edge)

eIDAS 2 file : Trust services
Attestations

What is it?

"electronic attestation of attributes' means an attestation in electronic form that allows the authentication of attributes"

Attestation on any type of data : **quality or characteristic** of the holder (address,..) and **rights/authorizations** of the holder (driving license,...)

Instrumental for the digital identity ecosystem shaped by the text

Non qualified or **qualified**

Non Qualified attestation (EAA)

No requirements on the format
No requirements of the very nature of the issuer
Legal aspects:

- No legal force
- No guarantee regarding the trust to put in the attestation

Qualified attestation (QEAA)

Requirement on the format (set of data signed)
Shall be issued by a Qualified Trust Service Provider
A minimum SLA is required for the revocation
Legal aspects:

- Same legal force as lawfully issued attestation in paper form
- Protective liability regime as it is issued by a Qualified Trust Service provider

eIDAS 2 file : Trust services
Updates for trust services providers

Cybersecurity requirements

All trust services shall abide by technical and organizational measures pursuant to NIS2 directive

Liability regime remains unchanged

Non qualified

-Supervision ex post

Qualified

-Supervision ex ante

-Mandatory conformity assessment to confirm its meets the applicable requirements

-Liability regime : "***The intention or negligence of a qualified trust service provider shall be presumed*** "

Updates for qualified trust service providers

Rules for verification of holder's identity

Clarification of supervision

Also entitled to issue qualified attestation

eIDAS 2 file : Trust services
3 new qualified trust services

What is it?

Provided by a qualified trust service provider

Meets the applicable requirements defined in the regulation

Compliancy with applicable requirements shall be verified by a conformity assessment body

Which benefits?

Protective liability regime for the user as it is issued by a Qualified Trust Service provider

Legal effects : the outcome of a qualified trust service enjoys in court the presumption of conformity to the corresponding properties

Validation service for qualified electronic signatures/seal

Preservation service for qualified electronic signatures/seal

Electronic time stamps

Electronic registered delivery services

+

Electronic archiving services

Electronic ledgers

Management of remote electronic signature and seal creation devices

eIDAS 2 file : Trust services
Qualified trust service : Focus on Electronic ledgers

Legal definition

Defined in a technology neutral manner and may be achieved in various technical manner (repository, blockchain,..)

Shall meet the following properties:

- Integrity of record
- Accuracy of chronological ordering

May be used across various sectors as a building block

Legal effects of qualified electronic ledgers

1/**Identification** of the origin of data records in the ledger (who wrote it)

2/**Unique sequential chronological ordering** of data records

3/**Integrity** of data records

=> Technical standards and assessment methodology needed

Executive summary

1. **About Eurosmart : a strong track record in cybersecurity & digital identity**

2. **eIDAS 2 file**
   - Overview
   - Digital identity
   - Trust services

3. **eIDAS 2 file : Cybersecurity aspects**

4. **Conclusion**

eIDAS 2 : Cybersecurity aspects

The text sets high level of expectations regarding cybersecurity for

- The wallet and wallet issuer
- Electronic identification scheme (under which the wallet is issued)
- Trust services

Including as well data protection requirements for

- Wallet and wallet issuer
- Providers of attestations

eIDAS 2 : Cybersecurity aspects
Wallet and wallet issuer

Cybersecurity

Obligation of cybersecurity certification of the Wallet pursuant to the Cybersecurity Act (regulation 2019/881)

List if cybersecurity schemes and supporting documents to be used will be defined later

Mandatory vulnerability assessment every two years

Obligation for the wallet issuer to continuously maintain the security of the wallet. Obligation of suspension or revocation of the wallet should a security breach occurs.

Data protection

Obligation of certification to ensure the data protection measures are met

- Selective disclosure
- Logical separation of data
- …

Does not replace compliancy to GDPR

eIDAS 2 : Cybersecurity aspects
Electronic identification scheme

Cybersecurity

Obligation of cybersecurity certification of the Electronic identification scheme pursuant to the Cybersecurity Act (regulation 2019/881)

- Includes issuance, management, mechanisms for authentication/validation of wallet

Mandatory vulnerability assessment every two years

Parts of electronic identification scheme that have been security certified do not have to go through peer review

Obligation for the Electronic identification scheme to continuously maintain the security of its infrastructure. Obligation of suspension or revocation of authentication service should a security breach occurs.

eIDAS 2 : Cybersecurity aspects
Trust services

Cybersecurity

For all trust services : compliancy with cybersecurity requirements defined by NIS

For non-qualified trust services : compliancy with cybersecurity requirements defined in the text shall be met

For qualified trust services : compliancy with cybersecurity requirements defined in the text shall be verified as part of the conformity assessment

Data protection

For providers of attestation : compliancy with data protection requirements defined in the text shall be met

Verification ex ante for providers of qualified attestation, ex post for providers of attestation

eIDAS 2 : Cybersecurity aspects
Many open issues still to solve….

Cybersecurity certification under the Cybersecurity Act (regulation 2019/881)

Current status of certification schemes

- Only three security schemes under preparation (Common Criteria, Cloud, 5G) for more than a year

Certification will require several other cybersecurity schemes

- Facial biometry for wallet activation, provisioning of identification data on the wallet…
- Software on mobile phone…
- Distributed ledger….

Which security level for evaluation?

- “Substantial” or “high”?
- Is it acceptable not to target the highest level for such sensitive assets (electronic identity)?

Security certification on mobile

Some wallet features may require access to secure hardware to meet a high level of security. How to ensure free access?

How to maintain security in a mobile which is fast changing environment?

How to manage the topic of supply chain attacks?

Ledgers

Ledgers may also be employed to support implementation of digital identity infrastructure. The text gives legal existence to electronic ledgers and clarifies their legal effects, subject to certification

How to assess their security in the case of blockchain implementation?

Executive summary

1. **About Eurosmart : a strong track record in cybersecurity & digital identity**

2. **eIDAS 2 file**
   - Overview
   - Digital identity
   - Trust services

3. **eIDAS 2 file : Cybersecurity aspects**

4. **Conclusion**

Conclusion

This presentation only provides an overview of some issues at stake, as the text is very complex and rich

eIDAS 2 is a very ambitious initiative which is monitored worldwide

The full implementation of the digital identity framework is likely to take years

Major key challenges will have to be solved before its uptake (just to name a few)

- Business model
- Get independent from locked mobile phone's ecosystems controlled by gatekeepers
- Cybersecurity certification on mobile environment
- Data territoriality
- …..

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Eurosmart Cybersecurity and Digital Identity Committee (CDI)

Latest publications: https://www.eurosmart.com/committees-and-task-forces/cdi/

Eurosmart | Square de Meeûs 35 | 1000 Brussels | Belgium