eDelivery updates

3 November 2022

Agenda

1 Policy update

Transition from CEF to DEP
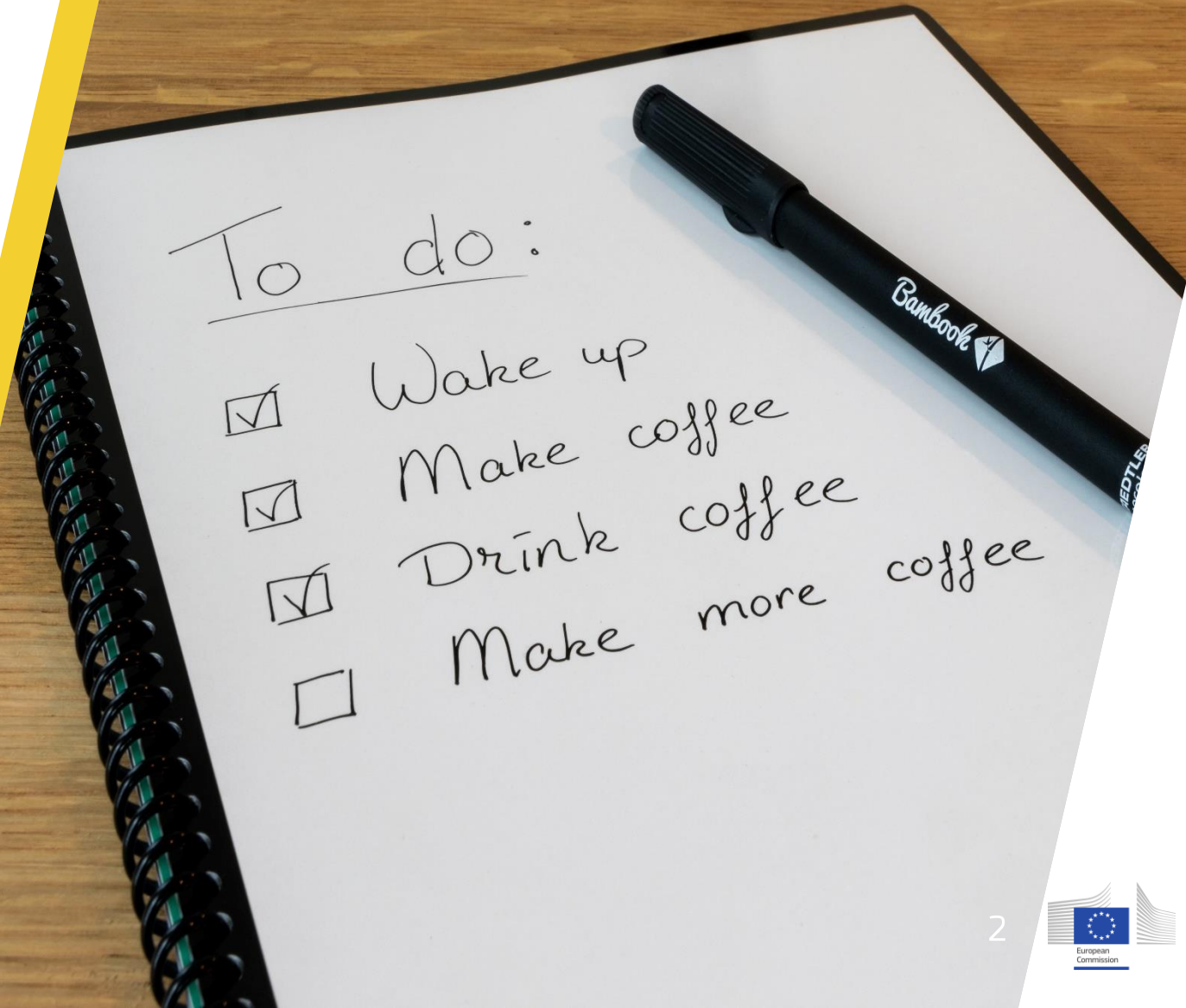
2 Funding update

eDelivery grants

3 Profile Update

Security changes to eDelivery AS4 profile

4 Stay tuned

eDelivery newsletters

Building Blocks Policy Framework

2014
Launch of the Connecting Europe Facility

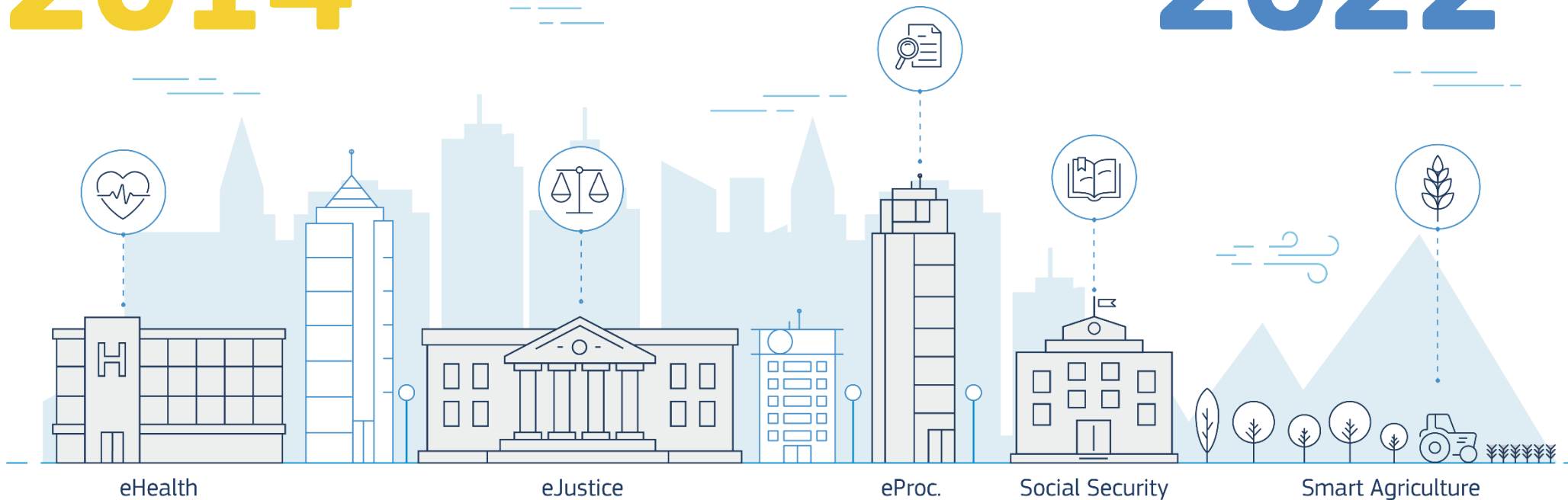## 2021
Launch of the Digital Europe Programme

2014-2020's Multiannual Financial Framework

2021-2027's Multiannual Financial Framework

Building Blocks adoption throughout the years & sectors

2014

2022

eHealth   eJustice   eProc.   Social Security   Smart Agriculture

- **338** projects reusing a Building Block.
- **53** projects committed to reuse.

- **88** projects committed to analyse.
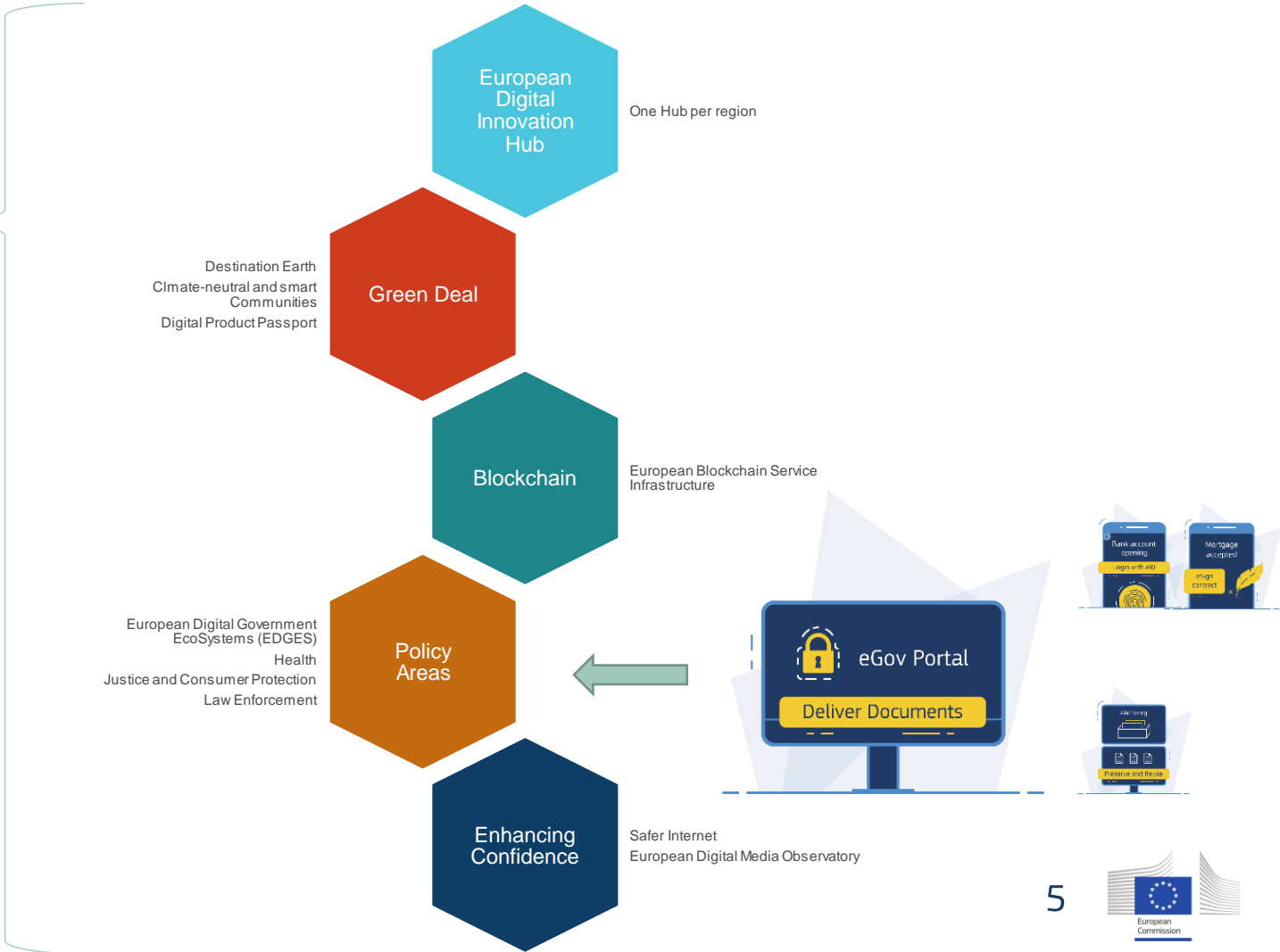- **150%** increase in reuse since 2018.

Digital Europe Programme – Specific Objective 5

Deployment and Best Use of Digital Capacities and Interoperability

Specific Objective 5 in WP 2021-2022

Investing in the future:
Digital Europe Programme

Other SOs relate to HPC, AI, Cyber and Digital Skills

European Digital Innovation Hub — One Hub per region

Green Deal
- Destination Earth
- Clmate-neutral and smart Communities
- Digital Product Passport

Blockchain — European Blockchain Service Infrastructure

Policy Areas
- European Digital Government EcoSystems (EDGES)
- Health
- Justice and Consumer Protection
- Law Enforcement

eGov Portal
Deliver Documents

Enhancing Confidence
- Safer Internet
- European Digital Media Observatory

5

European Commission

EDGES

Continuation of CEF Digital + ISA² solutions

Data Ecosystem											Language Technologies	Architecture	Assessment			Policy supporting reusable solutions							Cross-domains reusable tools					Stakeholder Engagement
Trust		Service Metadata			Semantics					Data sharing							Infringement	Competition		Procurement						Methods		
eID	eSignature	Registry of Authorities	Evidence Broker	Data Service Directory	CoreVocs (SEMIC) / CPSV-AP	Access to Base Registries	VocBench3	GeoData specifications (ETF testing framework +Re3gistry)	Electronic Documents and Electronic Files	eDelivery	eTrustEx	Automatic Translation	European Interoperability Architecture (EIA)	IMAPS (Interoperability Assessment of Digital Public Services)	CAMSS	Interoperability Testbed	THEMIS	eLeniency/eConfidentiality / eRFI	Electronic access to EC documents	eInvoicing	eCertis, ESPD (eProcurement)	Alignment of the former ESPD with the eProcurement Ontology, eForms and other services	Circabc	Eusurvey	LEOS	REF2LINK	European Legislation Identifier (ELI)	Joinup - 2016.20	Support to the platform / Stakeholder

6

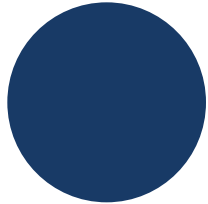# eDelivery 2014-2020

CEF Telecom Programme

Grants

Results

- 6 calls for grants, last one in 2020

- Budgets between €500k and €1M

- Last eDelivery action ended in September 2022

- 23 grants contracted

- 63 Access Points deployed

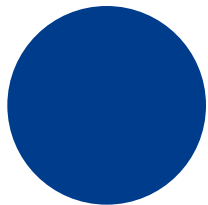- Total EU budget €5.16M with total costs of €6.95M in 19 MS, 2 EEA countries and one former MS (UK)

# eDelivery 2021-2027

What's next for eDelivery grants?

No specific funding

Specific funding for eDelivery is no longer available at the European level.

Funding as part of larger actions

Funding of eDelivery-related work may be eligible as part of larger actions under call priorities established in a Digital European Programme Work Programme, especially if under Specific Objective 5.
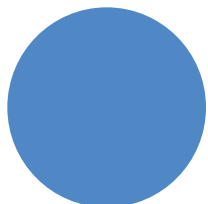
Funding at national level

Funding may be available from specific Member States as part of the national call for proposals using EU funds (NextGenerationEU).

Security changes to eDelivery AS4 profile

Objectives

New cryptography

Update cryptographic primitives to switch from RSA-based algorithms to more modern/secure ones (EC-based)

Better security

Define optional security enhancement to enable Perfect Forward Secrecy for eDelivery encryption

Updated TLS recommendations

Review and update the eDelivery recommendations concerning the use and configuration of TLS

Updated SMP specifications

Update the SMP specification to allow parties to publish metadata that can allow a gradual migration to the new cryptography

New cryptography: migrate away from RSA

Algorithm/Scheme	Proposal
Block Cipher	AES
Hash Function	SHA-2 family
AEAD	GCM/AES
Key Derivation Function	HKDF
MAC	HMAC/SHA-2
Digital Signature	EdDSA
Certificate Verification	RSASSA-PSS, RSA PKCS1-v1_5, ECDSA
Key Agreement	ECDHE
Key Transport	RSAES-OAEP
Key Encapsulation	ECIES-KEM

+ **ECDSA**

Already supported by eDelivery AS4 profile

To be supported by eDelivery AS4 profile

Not used

Design to avoid "big bang" switch from old to new cryptography (allow networks to transition gradually)

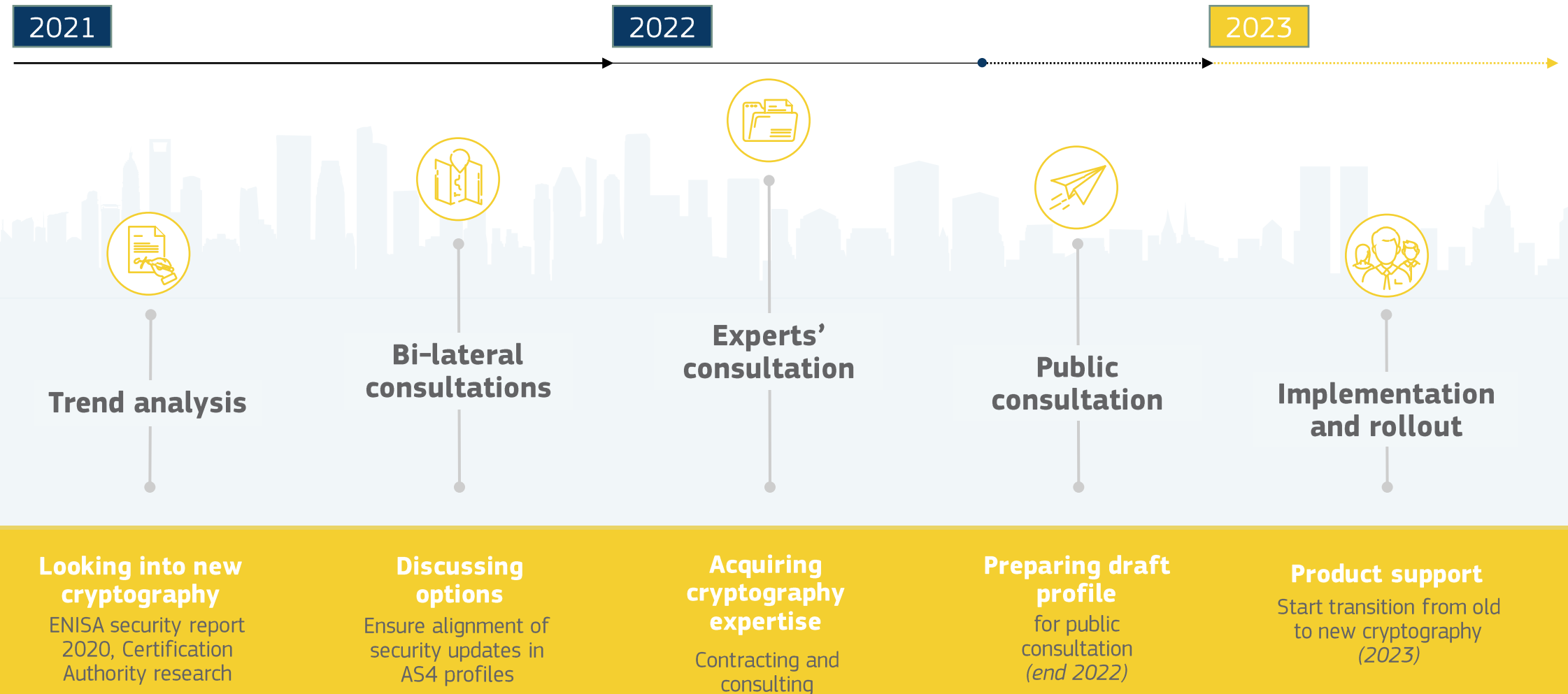# Updated SMP specifications

Objective

- Co-existence of RSA and EC metadata

- Tentative: publish separate certificates for signature and encryption

- Ensure backwards compatibility

Approach

- Use of multiple SMP transport profiles

- Adopt SMP 2.0

- No changes to current transport profile
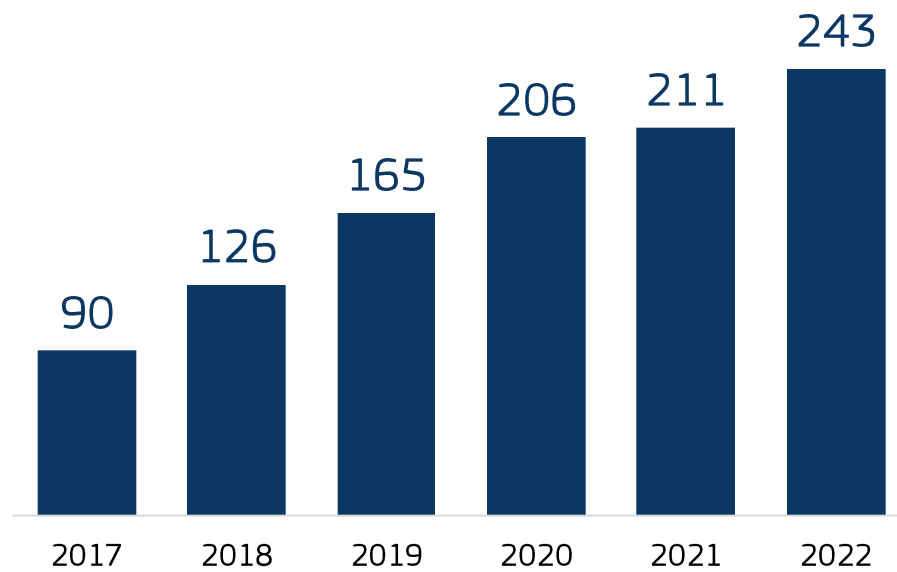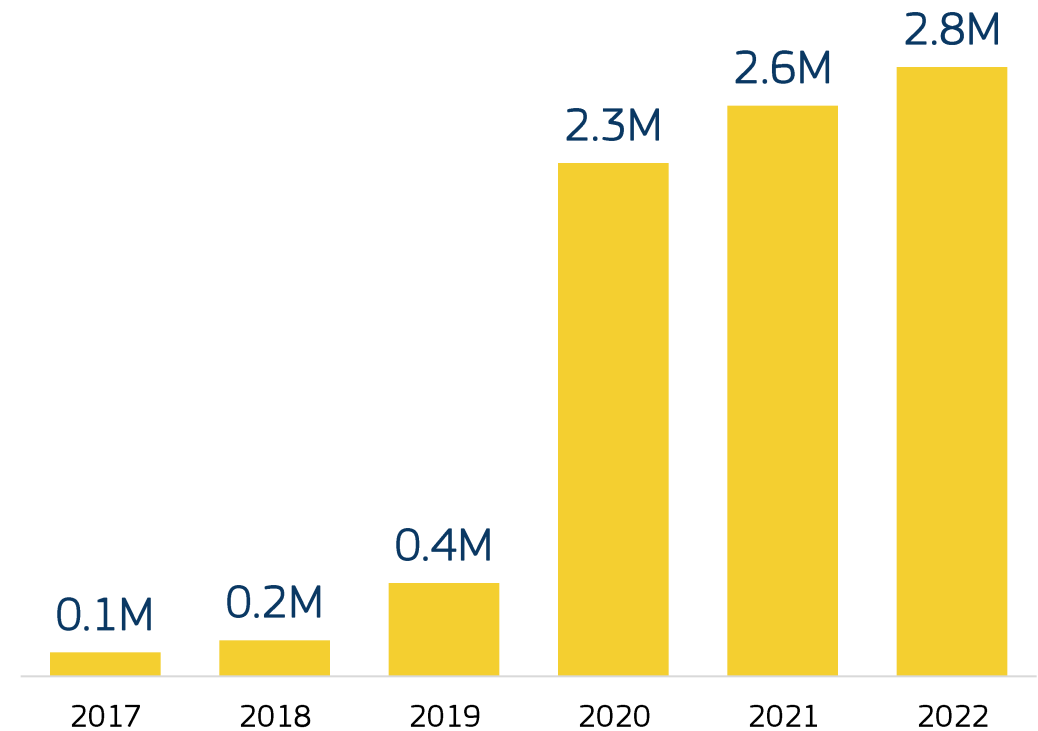
Security changes to eDelivery AS4 profile

Roadmap

2021   **2022**   **2023**

Trend analysis

Bi-lateral consultations

Experts' consultation

Public consultation

Implementation and rollout

Looking into new cryptography

ENISA security report 2020, Certification Authority research

Discussing options

Ensure alignment of security updates in AS4 profiles

Acquiring cryptography expertise

Contracting and consulting

Preparing draft profile

for public consultation *(end 2022)*

Product support

Start transition from old to new cryptography *(2023)*

SML Service use

Statistics since 2017

Number of connected SMPs

Number of registered participants

Number of connected SMPs:
- 2017: 90
- 2018: 126
- 2019: 165
- 2020: 206
- 2021: 211
- 2022: 243

Number of registered participants:
- 2017: 0.1M
- 2018: 0.2M
- 2019: 0.4M
- 2020: 2.3M
- 2021: 2.6M
- 2022: 2.8M

Publications

Feel free to register here

eDelivery (4x/year)

https://europa.eu/!v4njKB

Building Blocks (2x/year)

https://europa.eu/!jj87JU

Events

Success stories

News

Technical Updates

Find out more about

eDelivery

Thank you!

Click the link:

https://europa.eu/!8rtpfj

https://europa.eu/!HkhvPD

Drop us a line:

Bogdan Dumitriu
Project officer

Bogdan.DUMITRIU@ec.europa.eu.com
EC-DIGITAL-BUILDING-BLOCKS@ec.europa.eu