ROSATOM

TRUSTED SERVICES PLATFORM

Directorate of cryptographic security and trusted IT-services

Trusted Services Platform

ROSATOM

TPS is the nuclear industry system and IT infrastructure for accounting of cryptographic protection of information and work with electronic signatures

GEN.43 — Maintenance of an account with an electronic signature

Security Administrator OKZ

GEN.23

CLB.21 — Assessment of the level of trust

CLB.32 — Integration support for TSP

CLB.11 — Corporate Certifying

"VIPNET-GreenAtom" Complex

CLB.26

CLB.23 — Trusted services platform

CLB.18 — Орган криптографической защиты

CONVENIENT

- Obtain and renew digital signature certificates without visiting the certification center

- Work in corporate information systems without installing additional software

SECURE

- Transparency of using digital signatures and CIPF*

- Increased level of control over the use of digital signatures

501 organizations / enterprises

86 393 users

HOW TO JOIN?

To get access to the Trusted Services Platform, conclude an agreement with the TSP Operator and specify the required scope of subscription services
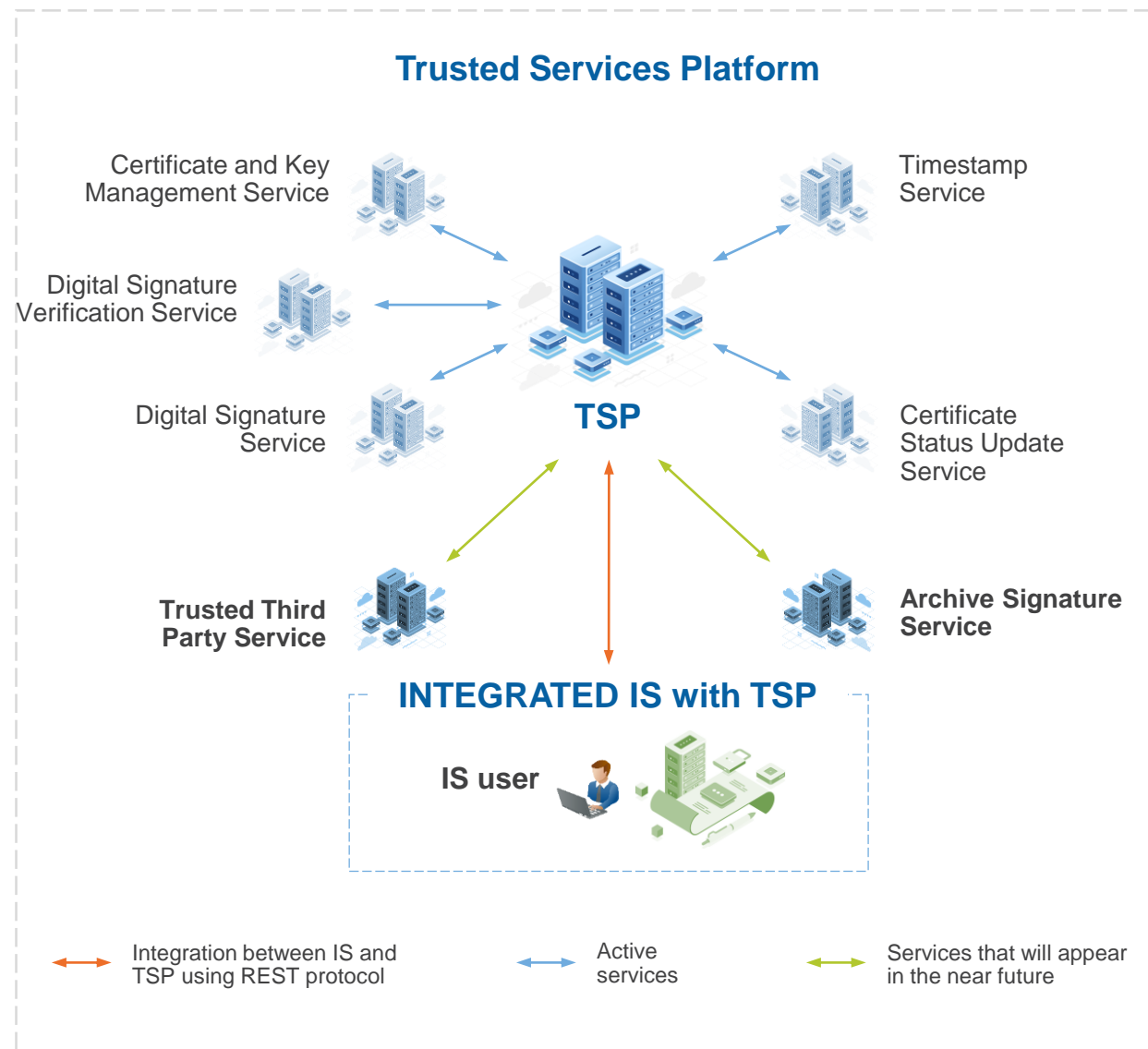
Website

Email

SYSTEM TASKS:

01 Action:
Create an infrastructure of trusted services for the use of electronic signatures in ROSATOM corporate information systems

02 Consequences:
Trusted services that ensure the legal significance of electronic document management, get unified and centralized

03 Countermeasures:
Implement compliance with the requirements of federal legislation, by-laws, regulatory requirements when using a digital signature

*CIPF – Cryptographic Information Protection Facility

TSP services: Digital signature

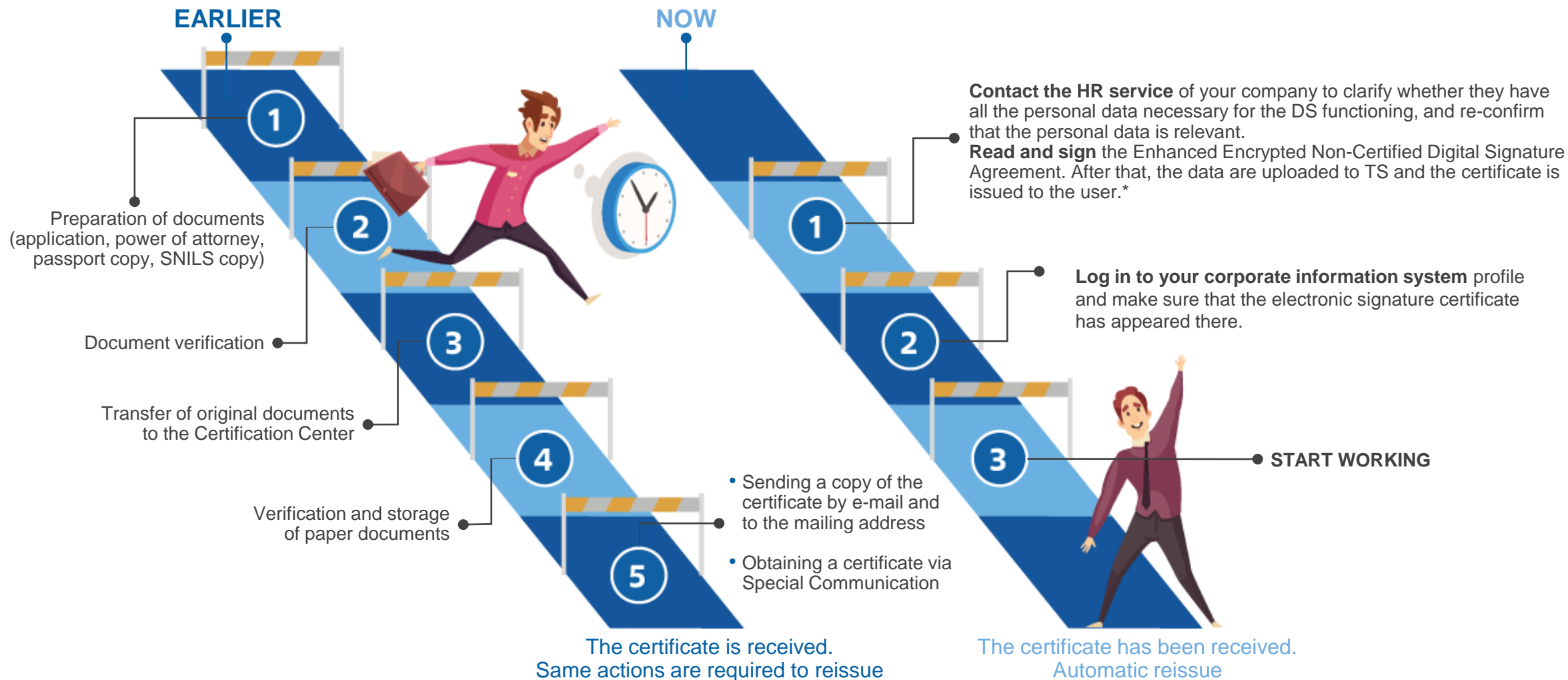## INTEGRATED INFORMATION SYSTEM WITH TSP PROVIDES:

- **Certificate and Key Management Service** – issues digital signature verification key certificates.

- **Digital signature service** – forms digital signatures in an improved format (CAdES with Extended Long validation data Type 1 (CAdES-X Long Type 1)).

- **Digital signature verification service** – verifies certificates (expiration date, chain of trust, revocation) and performs the verification procedure to ensure the authenticity of digital signatures of documents in various formats.

- **Timestamp service** – indicates the date and time, following TSP (Time-Stamp Protocol).

- **Certificate Status Update Service** – sets the status of certificates based on the OCSP (Online Certificate Status Protocol).

- **Archive signature service (to be implemented in 2025)** – provides prolongation of digital signatures in document management systems for long-term archival storage (more than 10 years)

- **TTP service (to be implemented in 2025)** – confirms the validity of digital signatures and certificates, verifies the credentials and records the verification result in the form of a receipt signed/certified by TTP services.

Trusted Services Platform

Certificate and Key Management Service • Timestamp Service • Digital Signature Verification Service • Certificate Status Update Service • Digital Signature Service • **TSP** • Trusted Third Party Service • **Archive Signature Service** • **INTEGRATED IS with TSP** • **IS user**

Integration between IS and TSP using REST protocol | Active services | Services that will appear in the near future
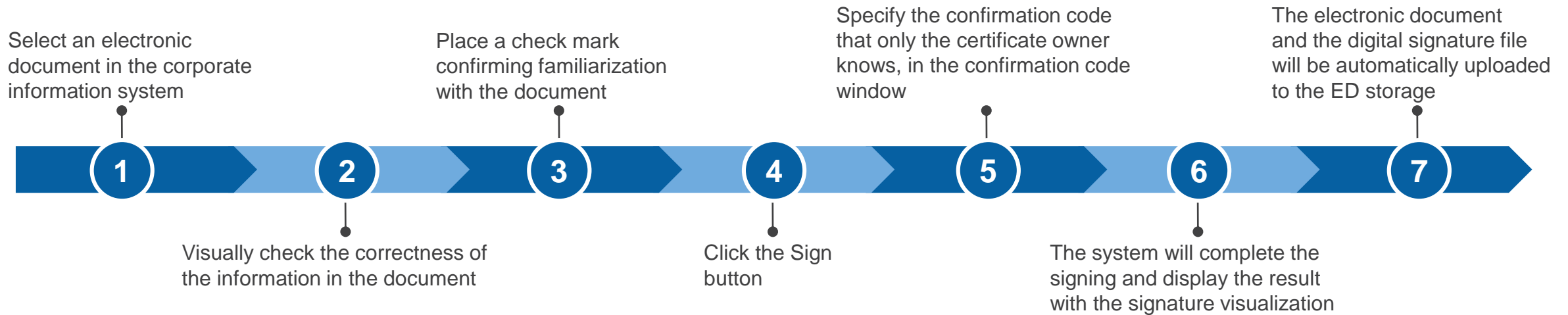
3

Enhanced encrypted non-certified digital signature: How to get one

ROSATOM

OBTAINING A DIGITAL SIGNATURE IS VERY EASY—THE PROCESS IS ALMOST COMPLETELY AUTOMATED.

There is no need to install additional software on your computer or plugins to your browser.
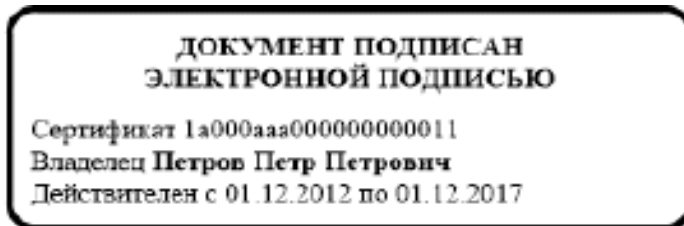
EARLIER

1 Preparation of documents (application, power of attorney, passport copy, SNILS copy)

2 Document verification

3 Transfer of original documents to the Certification Center

4 Verification and storage of paper documents

5
- Sending a copy of the certificate by e-mail and to the mailing address
- Obtaining a certificate via Special Communication

The certificate is received.
Same actions are required to reissue

NOW

1 **Contact the HR service** of your company to clarify whether they have all the personal data necessary for the DS functioning, and re-confirm that the personal data is relevant.
Read and sign the Enhanced Encrypted Non-Certified Digital Signature Agreement. After that, the data are uploaded to TS and the certificate is issued to the user.*

2 **Log in to your corporate information system** profile and make sure that the electronic signature certificate has appeared there.

3 **START WORKING**

The certificate has been received.
Automatic reissue

4

Deterled signing process

ROSATOM

Steps in the Corporate Information system interface

Select an electronic document in the corporate information system

Place a check mark confirming familiarization with the document

Specify the confirmation code that only the certificate owner knows, in the confirmation code window

The electronic document and the digital signature file will be automatically uploaded to the ED storage

1 **2** **3** **4** **5** **6** **7**

Visually check the correctness of the information in the document

Click the Sign button

The system will complete the signing and display the result with the signature visualization

Visualization of the document signing mark

The result of the process is an electronically signed document with a signature mark at the bottom of the document. Example and description of the mark fields.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат 1a000aaa000000000011
Владелец Петров Петр Петрович
Действителен с 01.12.2012 по 01.12.2017

✓ The text «The document is signed with an electronic signature»

✓ Number of the electronic signature certificate

✓ Full name of the owner of the electronic signature certificate

✓ Validity period of the electronic signature certificate

Corporate information systems integrated with TSP
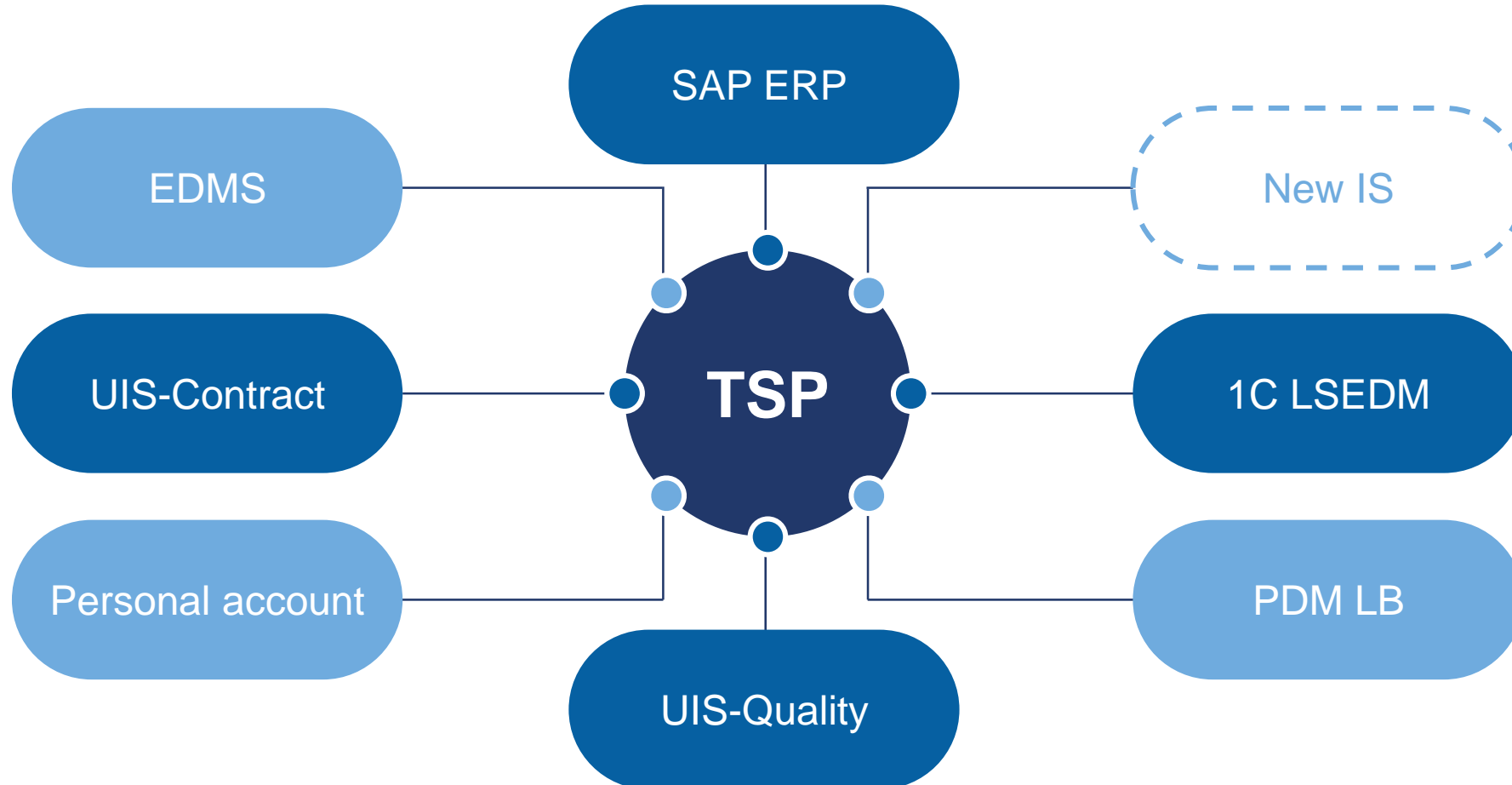
- TSP provides EECDS and EENCDS
- TSP is a universal centralized Service
- The new IS integrates with the TSP

Trusted Third Party services

ROSATOM

- **Confirmation of digital signature validity**
- **Verification of compliance of all qualified certificates used when signing an electronic document**

Documents are exchanged electronically using the proposed document management system that is common to companies, operating in the legal field of the Russian Federation, and a foreign counterparty. In case of application of this architecture, the recipient party will receive a receipt of foreign signature verification in the interface of the applied EDI in automatic mode. In the absence of the EDI, the recipient party will be able to check the foreign DS in the interface of the Trusted Services Platform.

Countries for which cross-border exchange of electronic documentation is possible:
Sweden, Germany, Turkey, Hungary, Czech Republic, China, United Arab Emirates, Republic of Korea, Republic of Belarus, Iran, India, Bangladesh, Egypt, Kazakhstan

Current use of Corporation's IS in international projects

Approval of document in IS
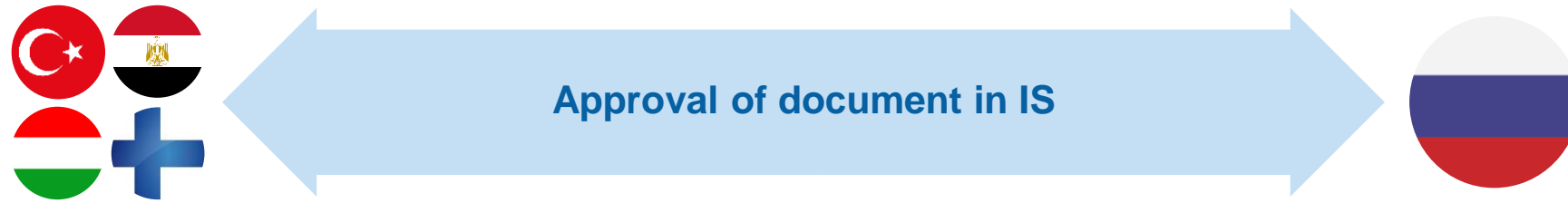
Current process:

Disadvantages of the current process:

- Additional expenses
- Temporary losses

- Risks of information manipulation
- There is no mutual recognition of ES* m/s by countries

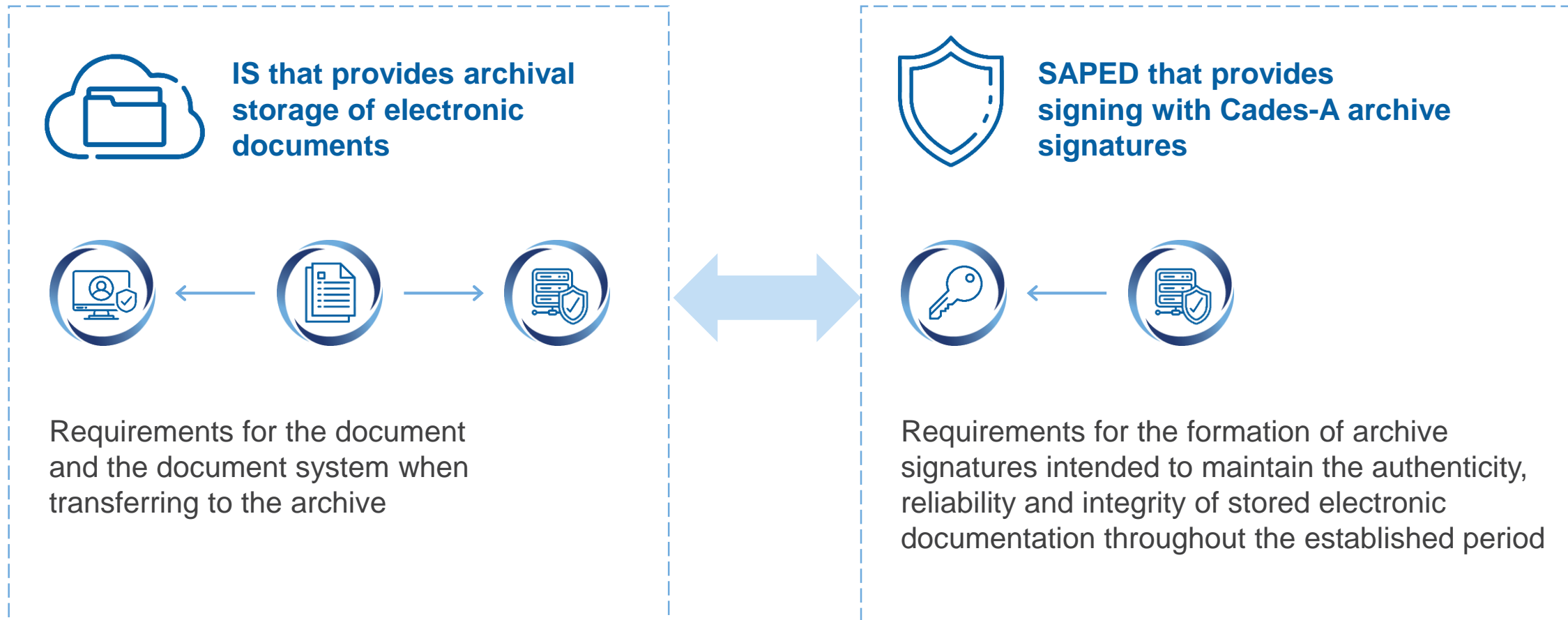- Risks of loss of documents
- There is no recognition of the Russian ES

Target process:

e-doc

*DS – digital signature

Archive Digital Signature for long-term storage (SAPED)

ROSATOM

IS that provides archival storage of electronic documents

Requirements for the document and the document system when transferring to the archive

SAPED that provides signing with Cades-A archive signatures

Requirements for the formation of archive signatures intended to maintain the authenticity, reliability and integrity of stored electronic documentation throughout the established period

Issuing and accounting of CIPF in TSP

✗

- Applications and accounting documents on paper
- Lack of centralized accounting of CIPFs
- Control over CIPF operation without specialized tools
- Labor-intensive user training process
- Lack of centralized exchange of operational documentation

✓

- Transfer of all processes to EDM
- Reducing the time of processes
- Interaction of ISA RSO (All-Russian Classifier of Occupations)
- Remote user training and online testing (WebSoft)
- Centralized management and control of CIPF (TSP Agent)
- Centralized accounting of CIPF
- Up-to-date information about CIPF 24×7
- Automatic preparation of CIPF accounting documents

>55% **labor savings due to automation and centralization of processes**

More about TSP

Contents

GREENATOM JSC
General Service Center of the State Atomic Energy Corporation Rosatom
Address: 115533, Moscow, Pervi-Nagatinsky Proezd 10 bld. 1
Tel.: +7 (499) 949 49 19
www.greenatom.ru
www.crypto.rosatom.ru