CRYPTOMATHIC

Electronic Signatures for Banking Operations in Russia - a benchmark with eIDAS

by Ivan Piskunov (guest) on 24. July 2017

Digital Signatures eIDAS

To read the Russian version of this article:

Электронная подпись и ее применение в России

This article examines the use of cryptographic means for information security, and in particular, the electronic signature. It focuses on the use of electronic security signatures (ESS) in various sectors, including the domestic use of cryptographic algorithms and requirements of the Federal Security Service of Russia (FSB) for hardware and software.

Additionally, attention is given to the European standard for eIDs, eTransactions, eSigning, and trust services (eIDAS) and the compliance of the local cryptographic certification authority and security product requirements.

The Central Bank of Russia sets requirements for both information security and the protection of payment information for all banks doing business in Russia.

STO BR IBBS is the Bank of Russia's industry standard for information security. It provides requirements for protecting critical business processes that are linked with financial transactions and personal customer data. This document addresses all the subsystems of corporate information security, which are divided into two large blocks of managing information security and technical requirements.

In the technical requirements, attention is given to such points as:

- Distribution of rights and roles of users
- Configuration of built-in protection mechanisms in automated banking systems (ABS)
- Access control and logging
- Virus protection
- Use rule resources of the Internet
- Processing of personal data

The Electronic Security Signature (ESS)

One of chapters of the STO BR IBBS standard is devoted to using means of cryptographic protection of information, including the "electronic security signature."

An electronic security signature on an e-document that complies with STO BR IBBS is considered a mandatory requisite for legally significant documents. The signature provides document properties such as:

- Protection against modification (simulation protection)
- Definition of authorship
- Protection against tampering of timestamp

Through ESS, it became possible to transition from paper recordkeeping to electronic document and data exchange via the Internet. According to the requirements of the Federal Security Service of Russia (FSB) and Special Service of State Security by Technical Means (FSTEC), all devices, including chips or USB-sticks used for ESS must comply with the Russian GOST standard.

Only Russian algorithms can be used to create and verify e-signatures (hashes). The use of foreign cryptographic software is prohibited. Exceptions are made only for those vendors (software development companies) that have been voluntarily certified by the FSB. Certification involves the transfer of source code containing algorithms to verify software for ESS. During the process, the source code is checked for undocumented features and the existence of any special backdoors in the code.

This is why banks, many commercial companies and the Russian government use only domestic software. An ESS that is used with payment orders, cash orders, payment requests and similar financial documents must be created according to the Russian GOST. Although GOST differ from global algorithm standards, they use analogues. For example, GOST 28147-89 is the mathematical base of the DES cryptographic algorithm.

However, automated banking systems and remote banking services use recognized international standards for cryptography. Asymmetric algorithms, Diffie-Hellman, El Gamal or RSA are used to establish a secure communication session and key exchange between the client device (laptop or smartphone) and public server of the Bank. Data transfer from one bank to another occurs through a secure VPN-channel encoded by IPsec or Russian GOST, which can be encapsulated, i.e. the so-called double encryption "tunnel-in-tunnel."

ESS is Open to the Public

The Russian Standard ESS is open to the public and described in GOST R 34.10-2012. Foreign developers can easily access it when needed to adapt their software to what is required by Russian law. In addition to the ESS data, GOST R 34.10-2012 is used in secure protocols such as TSL, HTTPS, XML Encryption and DNSSEC.

Three Types of ESS

Technically, ESS is legally divided into three types:

1. Simple ESS - Essentially usernames and passwords where the dataset does not uniquely identify the user, but still provides some protection. This is the easiest and least expensive option for ESS. Simple ESS is used to access email, personal accounts, certain websites, etc.

2. Enhanced unqualified electronic signature - A signature that uniquely establishes the authorship of the document and protects it from modification. Enhanced unqualified electronic signatures can be used in two-way electronic document workflow exchange.

3. Reinforced qualified electronic signature – A signature that uniquely establishes the authorship of a document and protects it from modification in a secure storage device such as a USB-stick. A reinforced qualified electronic signature is subject to the accredited and authorized certification authority. Such a signature can be used for accessing the website of Public Procurement and exchanging financial data with government agencies (i.e. tax office or pension fund) or private companies in Russia and abroad.

Russian Solution Based on eIDAS

Despite the fact that Russia is not included in the European Union, Russia adopted the EU Regulation No.910/2014 of 23 July 2014 (eIDAS) for electronic identification and trust services for electronic transactions in the European Single Market. The Russian solution for secure eTransactions is based on ***eIDAS*** – the regulation establishes a common standard for trust services, including electronic signatures, and provides a framework for multi-disciplinary e-business activities carried out between public authorities, companies and individuals in all European Union member countries.

eIDAS establishes European requirements for information security and protection systems. For example, you may store and use the key used for creating a qualified electronic signature on the server of the accredited provider of trusted services, the so-called *TSP (Trust Service Provider).* However, this provider must be an accredited TSP. There are a number of requirements for authentication that are supported by strict options. User authentication must be at least two-factor and it must occur directly on the server creating the signature.

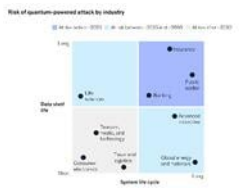
References and Further Reading

- Selected articles on Authentication (2014-16), by Heather Walker, Luis Balbas, Guillaume Forget, Jan Kjaersgaard, Dawn M. Turner and more
- Selected articles on Electronic Signing and Digital Signatures (2014-16), by Ashiq JA, Guillaume Forget, Jan Kjaersgaard , Peter Landrock, Torben Pedersen, Dawn M. Turner, Tricia Wittig and more
- REGULATION (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (2014) by the European Parliament and the European Commission
- Recommendations for the Security of Internet Payments (Final Version) (2013), by the European Central Bank
- Draft NIST Special Publication 800-63-3: Digital Authentication Guideline (2016), by the National Institute of Standards and Technology, USA.
- NIST Special Publication 800-63-2: Electronic Authentication Guideline (2013), by the National Institute of Standards and Technology, USA.
- Security Controls Related to Internat Banking Services (2016), Hong Kong Monetary Authority

Image: 0371 - Moskau 2015, courtesy of Uwe Brodrecht, Flickr (CC BY-SA 2.0 CC BY-SA 2.0)

Ivan Piskunov (guest)

RECENT



The NIST Announcement on Quantum-Resistant Cryptography Standards is Out. Act Now!

EMV Payment Security - Cardholders

Qualified Digital Signing: The Electronic Execution of Documents in England & Wales

MORE STORIES

SUBSCRIBE

The biggest stories, delivered to your inbox.

Enter your email here

SUBMIT

SHARE

FACEBOOK

TWITTER

LINKEDIN

E MAIL

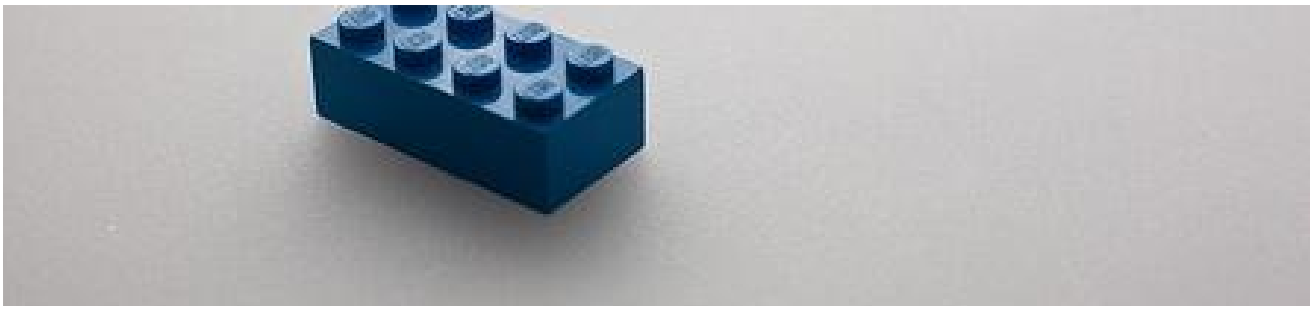
RELATED ARTICLES

Qualified Electronic Signing for Digital Mortgage Disruption and why a Wet Signature is ‘so last year’

Dawn Illing

UK eIDAS & EU eIDAS - What Does This Mean for Cross-Border Transactions and Digital Signatures?

Dawn Illing



How Cryptomathic Signer differs from other eIDAS compliant remote signing solutions

Thomas Pedersen

OTHER RELATED ARTICLES: # DIGITAL SIGNATURES # EIDAS

Want to know how we can help ?

Get in touch to better understand how our solutions secure ecommerce and billions of transactions worldwide.

CONTACT US

CRYPTOMATHIC

e: enquiry@cryptomathic.com

t: + 45 8676 2288

HEADQUARTERS

Aaboulevarden 22

8000 Aarhus C

Denmark

Company

Home

About Us

Solutions

Contact Us

Offices

Resources

News

Events

Blog

Resources