EUROPEAN CENTRAL BANK

EUROSYSTEM

Jere Virtanen

Market Infrastructure Management Division

Directorate General
Market Infrastructure and Payments

Endpoint security in TARGET2

Frankfurt, 4 December 2019

Overview

1. Compliance of TARGET2 with the CPMI Strategy
2. Implications for TARGET2 participants

Overview

Reducing the risk of wholesale payments fraud related to endpoint security

- Constantly **evolving threat landscape** and increasingly **sophisticated fraud attempts**; wholesale payments ecosystem is no exception
- May 2018: BIS Committee on Payments and Market Infrastructures (CPMI) publishes the report "Reducing the risk of wholesale payments fraud related to endpoint security" (hereinafter referred to as "**CPMI strategy**")
  - Focus on wholesale payment fraud
  - Definition of an endpoint: *"a point in place and time at which payment instruction information is exchanged between two parties in the ecosyste*m"
  - Each participant of a payment system and messaging network expected to bear primary responsibility for guarding against risk of fraud
  - CPMI strategy specifies seven elements RTGS operator should comply with

Compliance of TARGET2 with the CPMI strategy (1/5)

Element 1: Identify and understand the range of risks

- Endpoint security is a recurring topic in AMI-Pay and NSGs for creating awareness
- SWIFT as the single NSP: demonstrated ability to identify and understand the related risks
- TARGET2 participants deemed to have managed the risk stemming from allowing access to their account (TARGET2 Guideline, Annex II, article 28(5))

Element 2: Establish endpoint security requirements

- Annual TARGET2 self-certification arrangement
- Monitoring of TARGET2 participants' SWIFT CSP compliance

Compliance of TARGET2 with the CPMI strategy (2/5)

Element 3: Promote adherence

- Adherence against the TARGET2 self-certification arrangement
  - (Internal/external) auditor to sign the self-certification statement for critical participants
  - Endpoint Security Compliance Implementation Framework

Element 4: Provide and use information and tools to improve prevention and detection

- TARGET2 operator's expectation for participants to put in place adequate security controls (TARGET2 Guideline, Article 28(1))
- TARGET2 participants encouraged to making use of NSP or other service provider tools in addition to their own controls
- Fraud detection tool based on *ex post* reports available for Central Bank use

Compliance of TARGET2 with the CPMI strategy (3/5)

Element 5: Respond in a timely way to potential fraud

- Responsibility of timely fraud detection is on the TARGET2 participant
- SWIFT GPI will support payments tracking also in TARGET2
- TARGET2 participants' contact details available via the TARGET2 ICM for bilateral contact purposes
- TARGET2 participants are bound to inform its Central Bank in the event of security related incidents (TARGET2 Guideline, Annex II, article 28(2))
- Preparedness of TARGET2 Central Banks to secure a compromised participant's funds

Compliance of TARGET2 with the CPMI strategy (4/5)

Element 6: Support ongoing education, awareness and information-sharing

- Annual TARGET2 self-certification arrangement
- Use of SWIFT and other third party information sharing arrangements is encouraged

Element 7: Learn, evolve and coordinate

- Continuous revision of the TARGET2 self-certification arrangement
- SWIFT is reviewing the CSP
- TARGET2 operator is analysing security-related incidents that are reported by participants on an ongoing basis

Compliance of TARGET2 with the CPMI strategy (5/5)

Conclusion

- Self-assessment suggests that TARGET2 is largely compliant with the CPMI strategy
- Many elements have already been in place since the inception of TARGET2
- Recent actions taken to further increase the level of compliance
  - Extension of the TARGET2 self-certification arrangement to cover all participants
  - Monitoring of TARGET2 participants' compliance against the SWIFT CSP
  - Introduction of the Endpoint Security Compliance Implementation Framework
  - Dedicated (ex post) fraud detection tools
  - Preparedness of Central Banks to manage compromised participant's funds

Overview

Assurances from TARGET2 participants

TARGET2 self-certification arrangement

- **Information security** management requirements (all participants)
  - Covers back-office systems, internal networks and external network connectivity infrastructure
  - Requirements to be addressed in line with internationally recognized standards (ISO/IEC 27002)
- **Business continuity** management requirements (critical participants only)
- **Signature policy**: C-level executive + internal/external auditor (critical participants)

SWIFT Customer Security Programme

- TARGET2 Central Banks **request access** to their participants' self-attestation via the SWIFT KYC-SA.
- Focus on SWIFT CSP **mandatory controls**
- **SWIFT mandated assessment** (begun in 2018) and **Community standard assessment** as of 2020 onwards (independent external or internal assessment of self-attestation)

Compliance implementation (preliminary consideration)

- **Active Dialogue:** request for an action plan with dates for implementing corrective actions; inform supervisory authority of a non-compliant participant's status
- **Enhanced Monitoring:** participant reports regularly on the progress with the actions described in the action plan; Central Bank applies enhanced monitoring measures
- **Suspension:** all payments of a participant are queued in TARGET2 and the Central Bank will approve them individually
- **Termination of account**

+ Penalty charge?

	First stage implementation measures: 31 December of year *X*	Second stage implementation measures: 31 December of year *X + 1*
Broadly compliant participant (≥ 66% controls are satisfied)	**Active Dialogue** →	**Enhanced Monitoring**
Severely non-compliant part. (≤ 66% controls are satisfied)	**Active Dialogue + Enhanced Monitoring** →	**Suspension + Termination of account**

Compliance implementation (preliminary consideration)