**L2 >> L3 or tests name:** Cyber and IS Prevention >> Cryptography and PKI

**Legal entities in scope:** DBAG, ExR, EFAG, ECAG, CBF, CH, CBL, LuxCSD, CI, CS, CFCL and ECC/EEX

|  |
| --- |
| Cryptography and PKI (+covers AU-121-04-CSDR Cyber & IS) |

**Test(s) according to RCA:**

For Encryption and cryptographic controls, Cryptographic key management: DORA RTS- ICT RM - Articles 6 and 7 -(refer linked file in BCA under sub-section "Relevant legal and regulatory requirements" of section 5.3)

(TP1) IA to check SII 2024-040\_F06 status: - Lack of timely update and review of Cryptography Guideline (SII from previous audit 2024-040 Cyber and IS audit, Cryptography guideline document in Q3 2024 was replaced by new Data Security Guideline).

1.1 DE: Verify the performance of a timely update/review of the Cryptography Guideline / Data Security Guideline

1.2 DE: FuN 240708115004: Review the requirements provided in the new Data Security Guideline recently (that replaced Cryptography guideline document in Q3 2024).

(TP2) Obtain understanding if a policy has been established for the use of cryptographic controls. The policy should outline key requirements and appropriate controls e.g., for:

2.1 DE: Key Management and Certificate Management (Focus Topic)

-- Notable Incident (Blue/Non-CIF): April 3, 2025 - Certificate expiry incident. Azure secret, insufficient monitoring of secret expiration dates.

-- Special check if certificate expiry is holistically monitored or if this was limited to a certain area/product/platform

-- Guide question: Does DBG have insecure encryption protocols in use?

-- Guide question: Do we have an overview of the encryption status / gaps? Do we trust this data?

-- Check the utilization of methods for encryption at rest -> Expectation: should be implemented for strictly confidential data

-- Inspect the process for using Google-managed keys for cloud-based applications and evaluate if the risks are properly managed (i.e. is management accepting the risk of critical data not being protected by own keys?)

2.2 DE: Generation of keys (e.g. only using cryptographically secure random number generators, key length)

2.3 DE: Distribution of private keys (e.g. only encrypted and digitally signed)

2.4 DE: Storage of private keys (e.g. only in a dedicated securely encrypted area of the IT system; backup and archiving of keys only encrypted & digitally signed)

2.5 DE: Retrieval of keys (i.e. validation, requirements to retrieve a lost key)

2.6 DE: Retiring and destruction of keys (e.g. rotation, expiration requirements for keys)

2.7 DE: Audit logging requirements for key management activities

2.8 DE: HSM (hardware security module) - safeguarding digital keys

2.9 OE: PKI (setup & conformance) integration with applications/systems

2.10 DE: Post quantum cryptography resilience

-- Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant cryptography, is the development of cryptographic algorithms (usually public-key algorithms) that are currently thought to be secure against a cryptanalytic attack by a quantum computer.

-- Consider if such resilience has been duly considered to ensure the organisation is prepared for potential attacks on “old” credentials data once technology is readily available. (i.e., futureproofing)

(TP3) OE: For a sample of IT stack layers (e.g. network / servers / applications / ...), verify the usage of encryption and the respective parameters.

(TP4) For the applications to be covered as part of the L3 Cryptography and PKI, test for the following

4.1 DE/OE: IT security operation risks

-- Inspect the access rights granted to the application and verify the access rights are granted on a need-to-know/need-to-have basis.

4.2 DE/OE: IT availability and continuity risks

-- Obtain the Security Concept on the related IT Application and validate that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continuity.

-- Inspect the Security Concept and APMS whether RTO or RPOs are defined and in line with business needs.

-- Validate the adequacy of the Disaster Recovery Plan (if Availability=Critical)

-- Inspect relevant documentation whether any incidents occurred during the test on the applications in scope and if they were handled adequately and timely.

Covered Applications:

-- AID1064 - PKI DBAG

-- AID1065 - PKI MSCA

-- AID1066 - PKI Clearstream

5. Inspect relevant documentation whether any incidents occurred during the test on the applications in scope and if they were handled adequately and timely.

**Audit procedures/source:**

* Information directly requested from auditee (via e-mail or call) or extracted from provided documentation during preparation phase.

**Conclusion:**

Not ok, exception identified

Internal audit (KGF, ÖG) has performed the following Audit procedures:

**Summary of work done:**

**Note: From DORA Regulatory Technical Standards (RTS) on ICT risk management, IA performed the following tests in line with the requirements of Article 6 “Encryption and cryptographic controls” paragraphs 1-5 ( Refer to lines 10-14 on the sheet “RTS-ICT RM” in the document** [DORA Mapping to AU 2025.xlsx)](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/02%20Preparation%20-%20BCA/DORA%20Mapping%20to%20AU%202025.xlsx?d=w2a4589721a874394b14bbf3af0281057&csf=1&web=1&e=eGholS) and in line with the requirements of Article 7 “Cryptographic key management” paragraphs 1-5 (Refer to lines 15-19 on the sheet **“RTS-ICT RM” in the document** [DORA Mapping to AU 2025.xlsx)](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/02%20Preparation%20-%20BCA/DORA%20Mapping%20to%20AU%202025.xlsx?d=w2a4589721a874394b14bbf3af0281057&csf=1&web=1&e=eGholS)

IA noted the following DORA requirements were not addressed neither in the old Data Security Guideline V 1.1 nor in the new Encryption & Key Management Guideline V1.0

* Operational guidance providing information on how to determine necessity to mandate encryption of data in use applying the conditional “where necessary” clause as required by DORA based on data classification and ICT risk assessment, and permissible methods to implement or omit such encryption (e.g., confidential computing)
* Lack of minimum requirements deficiency for the monitoring/notification of the key/certificate expiration

However, IA didn’t raise a finding due to:

* The data security guideline published on the date 15/07/2024 before the date DORA became applicable
* the open S3 finding under the 2024-063 Technology Governance audit addressing procedures to be published by December 2026

Future Note: IA raised a future note (FuN number 250804132510) recommending that this area be revisited in the next audit cycle to evaluate whether the first LoD procedures are covering the DORA requirement pertaining to encryption for data in use & key/certificate monitoring.

Coverage result: OK with Future Note

|  |  |  |
| --- | --- | --- |
| **AP** | **Work done** | **Result** |
| **TP1** | IA to check SII 2024-040 F06 status: - Lack of timely update and review of Cryptography Guideline (SII from previous audit 2024-040 Cyber and IS audit, Cryptography guideline document in Q3 2024 was replaced by new Data Security Guideline).  **1.1 DE: Verify the performance of a timely update/review of the Cryptography Guideline/Data Security Guideline**  Observation: The guideline was replaced with the ICT Guideline “Encryption and Key Management v1.0” from Jan 17, 2025. As for the audit, there is no need to perform a yearly review, nor are there indicators that this document will not be reviewed in the next cycle.  **1.1 Conclusion: OK**  **1.2 DE: FuN 240708115004: Review the requirements provided in the new Data Security Guideline recently (that replaced Cryptography guideline document in Q3 2024).**  Core function of the document is highlighted here – as derived from DORA:    Summary of the guideline’s requirements:   1. Procedure, Development and Governance 2. Selection and Implementation of Cryptographic Measures 3. Review, assessment and monitoring of cryptographic measures and products 4. Documentation of key and crypto measures 5. Protection of Data in Transit 6. Protection of Data at Rest 7. Protection of Data in Use 8. Key Management and Governance 9. Key Generation 10. Key Distribution 11. Key Installation 12. Key Storage 13. Key Renewal/Rotation 14. Key Backup and Archiving 15. ICT-related incidents involving cryptographic keys 16. Key deletion 17. Cloud-specific encryption requirements 18. Certificate validation requirements 19. Electronic Messaging Controls   Sample of guideline’s requirements showing DORA relevance, covered InfoSec protection goals and further details on specific PKI and CERT requirements:    Observation: The guideline contains references to DORA via the ICT Risk Mgt Framework, as well as ISO27002 as the basis for the requirements. Additionally, the requirements are mapped to 1 or more of the 4 InfoSec protection goals. Specific rules are defined for PKIs and CAs in use, with specific encryption standards to be met. No indicators of material deviations were observed.  **1.2 Conclusion: OK**  Further examination of the guideline contents done in TP2. | **OK** |
| **TP2** | Obtain understanding if a policy has been established for the use of cryptographic controls. The policy should outline key requirements and appropriate controls e.g., for:  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID1,2,3,4,8*  Scope of services:<https://businessjira.deutsche-boerse.com/servicedesk/customer/portal/16>  [Link to workflow instructions](https://deutscheboerse.sharepoint.com/:w:/r/sites/DCM/ISO/inh_public/Documents/Jira/Jira%20-%20SECBAU%20Project%20-%20Instructions.docx?d=we1ea18afe47e405782d1db24c10b4125&csf=1&web=1&e=djtWqA) for end users (last updated 2021)  IA conducted walkthrough meetings on 22 May and 28 May with Claudio Di Nardo, Information Security Engineer/ IT Security.  Samples of working instructions and “audit documents” examined:        IA requested evidence demonstrating how yearly review process was carried at the end of the year 2024 for core manual instructions/audit documents/procedures pertaining the cryptographic measures:    Sample of the reviews performed:    Observation: During walkthroughs IA noticed that several audit documents and work instructions were outdated. Changes and reviews were not tracked in the document change history. Approvals were similarly absent. The existing control does not adequately operationalize the review process (missing 5W1H, no deadlines). Finding raised. Refer to Finding 6:  Finding 6: During an inspection of the cryptographic key management processes of the PKI applications (PKI DBAG (AID1064), PKI MSCA (AID1065) and PKI CLS (AID1066)), Internal Audit observed that a majority of the processes were performed by the Security IT - Digitise, Evolve & Innovate team (SAO). Upon requesting the corresponding procedures/work instructions, IA noted the following:   * Upon request for a dedicated procedure or work instruction for Key Management, SAO referenced an “Audit Document”. This document did not correspond to a “written rule” (i.e., policy/guideline/procedure) as defined by the overarching Written Rules Framework Guideline. * The ‘Audit Document’ for Key Management lacked content requirements, e.g., Purpose, Objective and Basis of the document, Scope and Target Groups, Updated Review/Approval records (incl. Head of Section Approval), and publication in central DBG storage. * IA was informed that the ‘Audit Document’ was not only used by SAO but also by multiple IT Operations/Production Support teams as a key reference for the structure of their own key management procedures done in conjunction with the corresponding PKI asset.   Further inspection of the SharePoint site containing the written-rules framework used by SAO revealed that 19/37 cryptography-related procedure documents had not been visibly reviewed and approved in several years (between 2020-2023). There was no indicator if procedures found in SharePoint were still active or decommissioned.  While a yearly control to review documents was defined via a JIRA task (SECPKII-1063), the control did not adequately define a detailed control procedure (i.e., description of tasks alongside the ‘who, what, how, where, when, why’ framework of the ICS guideline) nor did it provide adequate evidence of its performance in the ticket. Similarly, adequate evidence of the control performance was not evident in the individual documents, with the last recorded modification more than a year ago.  **2.1 DE: Key Management and Certificate Management**  -- Inspect the process for using Google-managed keys for cloud-based applications and evaluate if the risks are properly managed (i.e. is management accepting the risk of critical data not being protected by own keys?)  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID1,2,3,4,8 ID15, ID17*   * **Delineation of Responsibility:**  A distinction between PKI Entities Keys and End Entities private keys is made. All guidance pertaining to key management etc. is only valid for PKI entities and keys managed centrally. As stated, Security IT is responsible for managing and distributing public keys only. * “We force everyone to generate private keys on their own side, for reduced exposure to transmission risks via communication channels. “ * This is generally due to the Bring-Your-Own-Key (BYOK) structure. However, exemption cases for clients who cannot generate their own keys – these are co-managed and are tracked. * Regarding key/cert management: ultimate responsibility (for the compliance with the guideline) supposedly lies with the Application/Key/Cert owners. The Security IT Team (Security IT - Digitise, Evolve & Innovate (U)) only coordinates the tasks with supporting platforms. * **Staffing & Continuity:** The area is mission critical, with dependencies particularly requiring quick reaction times for CERT incidents. Availability of tools and persons must be guaranteed via BCPs and DRPs. * **Procedures and Key Management:**   Most administrative tasks are automated via scripts run from a Bastion Host with technical users. Some PAM is required for elevated permissions to run specific jobs. Other jobs are automated and run on schedules (cron).   * Monitoring of automated job success / failure with notification & escalation procedures   IA obtained the following evidence in the walkthrough with the Security IT - Digitise, Evolve & Innovate (U) team, showing the automated job that verifies whether a key or certificate has been revoked through OCSP. (Online Certificate Status Protocol which is a method for verifying if a certificate has been revoked by querying a Certificate Authority (CA))  Here a cron job is visible that is set up to schedule a task to query the Certificate Authority's OCSP responder. **The revocation status of keys or certificates is verified using scheduled cron jobs that query OCSP responders and download CRLs. The server initiates the requests, and the responses are validated to ensure they are correct and up to date.**      **The screenshot below displays a test environment focusing on certificate revocation. It includes a section listing Certification Authorities (CAs) with details such as their names, validity periods, and links to their OCSP responders and CA certificates. In the pop-up window titled, metadata is seen from a CRL (Certificate Revocation List), including the issuer, update timestamps, signature algorithm, CRL number, and cryptographic identifiers. This setup supports automated revocation checks via cron jobs, where the system periodically queries OCSP responders or downloads CRLs to ensure that certificates have not been revoked and that the revocation data is current and valid.**    The terminal screenshot displays a list of **active cron jobs** used to automate various PKI-related monitoring tasks. These include:   * **Every 5 Minutes**:   + checkCDP\_TEST.sh and checkOCSP.sh: Scripts that likely check the availability and freshness of CRLs (CDP) and OCSP responses.   + A Python script (bau\_process.py) for PKI automation in the dev environment. * **Hourly (at minute 0)**:   + Monitoring the **age of CDP and OCSP responses** during specific hours (0–6 and 18–23) on the 7th of April. * **Every 3 Hours**:   + checkLDAP\_TEST.sh: Checks LDAP replication and CHL (Change Log) data.   + hsmchk.sh: Monitors the health of the Hardware Security Module (HSM).   + chkcrlexpiry.sh: Verifies the expiration status of CRLs. * **Additional 5-Minute Checks**:   + Multiple invocations of checkCDP\_TEST.sh with different parameters (-c cdpum, -c tdap, etc.), likely targeting different CDP endpoints.   All outputs are redirected to /dev/null, meaning logs are suppressed unless handled elsewhere. This setup ensures **continuous, automated validation** of certificate revocation mechanisms    The script below, checks whether the OCSP response from the server is valid and logs the result to ensure that certificates are not revoked and that OCSP responders are functioning correctly:    The screenshot below, shows the **monitoring dashboard** from the **"Service search App SG - PKI"**, which is used to track the health and performance of various PKI-related services and infrastructure components:    -- Notable Incident (Blue/Non-CIF): April 3, 2025 - Certificate expiry incident. Azure secret, insufficient monitoring of secret expiration dates. Special check if certificate expiry is holistically monitored or if this was limited to a certain area/product/platform   * The root cause of the incident was due to manual disconnection/deactivation on the end user side of notifications / alerts. No further indicators of systemic failure of the notification system. * As established in process walkthrough for key generation, setting a monitoring alarm/contact person is mandatory. (see above jobs for cron jobs for automated verification)   IA verified that there are cron jobs supporting automated revocation checks via cron jobs, where the system periodically queries OCSP responders or downloads CRLs to ensure that certificates have not been revoked and that the revocation data is current and valid. IA didn't raise a finding as IA was informed by Security IT - Digitise, Evolve & Innovate (SAO) team that there will be a Teams plugin implemented to send notifications in Microsoft Teams regarding encryption key expirations.  **OK, with future note (FuN: 250805084801): IA raised a Future Note to check if the new system’s workflow allows for the acknowledgement and escalation of alerts, to prevent manual override from the end user’s side.**  **2.2 DE: Generation of keys**  (e.g. only using cryptographically secure random number generators, key length)  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID9 Key Generation*  \* Bring-Your-Own-Key (BYOK) structure, exemption cases for clients who cannot generate own keys  IA noted that, how cryptographic keys need to be generated securely, who is responsible, and how the generation process is controlled; outlined in the guideline. As per the guideline,   * Keys should only be created with the intent of establishing an approved trust relationship and must be deleted if approval of the request has been denied or revoked. When keys used in the “Red segregation area2” are generated, at least two persons should be present and provide a formal documentation of the steps performed. * If users generate their own keys, they should be guided in generating key material, especially when they decide parameters or add randomness. * The key generation must be carried out using a secure cryptographic key generator. For key generation and random number generator, there is a referral to requirements of BSI TR 02102-1, 02.02.2024 and NIST SP 800-90A, 06.2015 for more detail and for the HSM solution, there is a referral NIST stating that keys must be generated using FIPS 140-2 certified HSM solution. * The security parameters of the keys must be chosen such that they provide the strength and quality demanded by the legal entity.   Note: In the guideline, there is not any requirement to maintain logs of all key relevant events (creation, use, deletion, access). However, in the data security guideline V1.1 which is still valid until the new IS procedures are published, it is forced that in case cryptographic keys are managed by the Asset Owners themselves, all operations must be recorded in a log and forwarded to a central storage. Refer to page 36 in [DBG\_GS\_Data\_Security\_Guideline v1.1 (7).pdf](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Governance/DBG_GS_Data_Security_Guideline%20v1.1%20(7).pdf?csf=1&web=1&e=BzipcX)  In the procedures carried by Security IT, as an exemption to BYOK, keys are generated via two possible procedures: Manual workflow via JIRA or Automated Request via API   * For JIRA: this is where exception cases are done (i.e., legacy encryption techniques). Contact persons and other base data are requested, prior to a ticket moving forward in workflow, fulfillment of the requirements is ensured. Set of encryption services/options are made available for the customer (application owner) * These are seen on the service portal: <https://businessjira.deutsche-boerse.com/servicedesk/customer/portal/16>  Observation: The customers and approvers „guide“ is out of date – last updated in 2021. Refer to Finding 6 * Service catalog offerings may include legacy non-compliant key generation, as an explicit deprecated service run for compatibility with legacy applications. * For API: this is done directly.   **2.3 DE: Distribution of private keys**  (e.g. only encrypted and digitally signed)  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID10 Key Distribution; ID11 Key Installation*  IA noted that in the guideline, the rules, controls, and security requirements to ensure the cryptographic keys are distributed securely, traceably, and only to authorized entities. As per the guideline:  \* We force everyone to generate private keys on their own side to reduce reliance on encrypted communication (BYOK)  \* Asymmetric Encryption  -- 2 Channel communication, keystore sent via one, decryption via another  \* Symmetric Encryption (Data in Cloud)  -- Data is generated in air-gapped Hardware Security Module (HSM)  -- “keyblob” is wrapped and pushed to cloud  -- Decrypted on cloud   * Private key distribution must be prevented to avoid exposure, if applicable. * Private key distribution process must be done in encrypted form, and it must be ensured that the private key is kept confidential during the process. * Public keys must only be distributed by authorized users for the establishment of approved trust-relationships, and established trust-relationships must be documented.   **2.4 DE: Storage of private keys**  (e.g. only in a dedicated securely encrypted area of the IT system; backup and archiving of keys only encrypted & digitally signed)  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID12 Key Storage*  *As per the guideline:*   * The keys must be stored such that the strength and quality demanded by the legal entity is provided. * Key-encrypting keys must be stored separately from data-encrypting keys. * Private keys should remain non-exportable or vaulted * In case cryptographic keys are managed by the Asset Owners themselves, all operations must be recorded in a log and forwarded to a central storage * Hardware storing key material must be protected from loss, theft, or damage by appropriate organizational and physical measures and they must be certified to be tamper-proof * If the key is used to protect data classified as “critical” with respect to confidentiality or the visible label of the data is “strictly confidential”, it should be stored on a hardware security module. * Access to Key Encrypting Keys must be protected using the multiple-eyes principle. * Access to systems storing key material must be limited to the need-to-know principle for authorized people. * Private keys must only be stored in encrypted form. * If the key is used to protect data classified as “critical” with respect to confidentiality or the visible label of the data is “strictly confidential”, it should be stored on a hardware security module.   **2.5 DE: Retrieval of keys**  (i.e. validation, requirements to retrieve a lost key)  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID14 Key Backup & Archiving*  As per the guideline,   * Cryptographic keys must be protected when backed up and/or archived, and the same level of protection as key storage must be provided for the backed up and archived data as well. * Keys must be deposited (respectively backed up and/or archived) when they are used for encryption, or, in case of a key loss, access to the encrypted data is still required. * It must be ensured that keys can be restored and clarified from whom the data can be accessed, and the keys must be recoverable to quickly re-establish products and to access encrypted information in case of a disaster or media failure * Processes should be provided on how to react in case of a key loss or failure, malfunction, or breakdown of cryptographic products.   **2.6 DE: Retiring and destruction of keys** (e.g. rotation, expiration requirements for keys)  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID13 Key Renewal/Rotation; ID16 Key Deletion*  \* Asset owner via self-service portal determines the notification period  As per guideline,   * To address potential compromise of key material over time, a periodic key renewal should be performed. * For each use of cryptographic measures, the validity period of keys should be determined. * The process to renew keys should be initiated early enough to ensure that a new key is in place before the old key expires, and the new key should be independent from the previous key. * SSH-key pairs held by a group of individuals should be changed whenever an individual is removed from the group, and session keys should be changed after a specific time or number of encrypted packets, considering risk analysis. * Certificates must be renewed at an appropriate time before they expire.   **2.7 DE: Audit logging requirements for key management activities**  In the previous “Data Security Guideline”, on page 36, it is outlined that in case cryptographic keys are managed by the Asset Owners themselves, all operations must be recorded in a log and forwarded to central storage.  **2.7 Conclusion: OK – IA noted that the audit logging requirements for key management activities are defined in the Data Security Guideline.**  **2.8 DE: HSM (hardware security module) for safeguarding digital keys**  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID9 Key Generation*  -- Guide question: what certifications/requirements have we defined for our HSMs?  \* previously recorded hardware faults (manufacturer errors) in HSMs (>3 years ago) resulting in downtime, now we have 3 units instead of 2  \* reduction of on-premises hosted services, potential for using cloud based HSM  As per guideline,   * For major and critical IT assets the key generation should be done inside existing on-premises hardware security modules (HSM), and the keys are then synced to the CSP key storage solution. * It should be prevented that deleted keys can be recovered by any party in case keys are stored in a Hardware Secure Module (HSM).   **2.9 OE: PKI (setup & conformance) integration with applications/systems**  *REQ: Encryption & Key Mgt. Guideline v1.0 – ID8 Key Mgt.; ID9 Key Generation; ID10 Key Distribution; ID12 Key Storage; ID13 Key Renewal/Rotation; ID15 ICT Incidents; ID16 Key Deletion; ID18 Certificate Validation*  \* Rapid7 as primary detection tool  IA was informed that Corporate IT is responsible for managing and distributing public keys.  See TP 3.2 for operating effectiveness testing based on applications.  **2.10 DE: Post quantum cryptography resilience**  -- Post-quantum cryptography (PQC), sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant cryptography, is the development of cryptographic algorithms (usually public-key algorithms) that are currently thought to be secure against a cryptanalytic attack by a quantum computer.  -- Consider if such resilience has been duly considered to ensure the organization is prepared for potential attacks on “old” credentials data once technology is readily available. (i.e., futureproofing)   * While there are no concrete controls of PQC in place, the Security IT team has made initial evaluations of potential quantum-resilient solutions and algorithms. * Examples of design documents * Suggestions of PQC measures * The following external references (possibly future benchmarks) are being used for inspiration. <https://bouncycastle.org/>   **Conclusion: Not Ok. Finding raised. The "Encryption and Key Management Guideline" (Version 1.0, valid from 17.01.2025) outlines the control requirements for managing encryption and cryptographic keys within DBAG and its adopting Legal Entities. The Guideline serves as a comprehensive reference document, outlining the following fundamental components of encryption and key management: Cryptographic Measures, Review & Monitoring (annual reassessment of cryptographic tools), Documentation of PKI architecture, key registers and usage logs; Encryption needs for data in transit, data in use and data at rest; Key Management Lifecycle; Incident Handling; Certificate Validation and Electronic Messaging.**  **At the time of audit fieldwork, the responsible Corporate IT’s Security IT - Digitise, Evolve & Innovate (U), process document did not correspond to a “written rule” (i.e., policy/guideline/procedure) as defined by the overarching Written Rules Framework Guideline. Also, it did not follow a regular review/approval process. > See finding 6:** Deficiencies in cryptographic key management documentation and process governance. |  |
| **TP3** | **OE: For a sample of IT stack layers, verify the usage of encryption and the respective parameters.**  **3.1a – Big-picture-analysis of all AIDs with open ISRM encryption risks**  562 Applications were drawn from APMS and cross-referenced to ISRM tickets. The original raw exports from 05.06.2025 can be found here:   * APMS: [Applications.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Applications.xlsx?d=w6b3ecfbcbc5c459a8c045d56a67e7a74&csf=1&web=1&e=pJ1I8U) * VMT: [Vulnerability Management Tool & Risk Register 2025-06-04T15\_14\_18+0200.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Vulnerability%20Management%20Tool%20%26%20Risk%20Register%202025-06-04T15_14_18+0200.xlsx?d=w1e2c8a901a7b4b9b9df7b36472d09c61&csf=1&web=1&e=mMOPRH)   The data was parsed and mapped in [OE - Applications Sample.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/OE%20-%20Applications%20Sample.xlsx?d=w30b1c72c4ff3445aad91d0d87db94ef5&csf=1&web=1&e=3337zp), where the applications were classified as:   * ! – Active Risk: App has an open violation against control A.10.1.1 Cryptography, * O – Past Risk: App had a cryptography risk in the past that is now resolved. * X – Never: App had never been identified for a violation against cryptography   User Instructions:  Extract the AIDs from the ISRM tickets and consolidate to unique AIDs – ignore all other ID types with this function:  Column 1  *=MID(AU2,SEARCH("> ",AU2)+2,100)*  Column 2 *=UNIQUE(FILTER(AV2:AV726,LEFT(AV2:AV726,LEN("AID"))="AID","nope"),FALSE,FALSE)*  Extract from APMS all operational Apps, reference the exclusion list and filter out affected apps with this code:  =MATCH(B2,'Exclusion List'!$B:$B,0)  In summary, across all types of application hosting arrangements:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Row Labels | X - Never | O - Past Risk | ! - Active Risk | Grand Total | | Critical | 82 | 84 | **34 (17%)** | 200 | | Major | 118 | 34 | **18 (11%)** | 170 | | Minor | 70 | 21 | **11 (11%)** | 102 | | Negligible | 75 | 11 | **4 (4%)** | 90 | | Grand Total | **345** | **150** | **67 (12%)** | 562 |   Specifically, for on-prem or hybrid hosting arrangements, where DBG would have more direct control of the encryption state:   |  |  |  |  |  | | --- | --- | --- | --- | --- | | Row Labels | X - Never | O - Past Risk | ! - Active Risk | Grand Total | | Critical | 53 | 69 | **31 (20%)** | 153 | | Major | 84 | 29 | **14 (11%)** | 127 | | Minor | 44 | 17 | **9 (13%)** | 70 | | Negligible | 46 | 6 | **2 (4%)** | 54 | | Grand Total | 227 | 121 | **56 (14%)** | 404 |     **3.1b – Deep dive into the affected 31 Critical Applications with active risks (20%)**   |  |  |  |  | | --- | --- | --- | --- | | Application Name | APMS  AID | Issue Age  (Years) | IA Comments | | T7 | AID011 | **5** | **3xR3, 2xR2**  Continuously avoided/reassessed since 2020. Currently accepted risk in 2024 is rated R3 | | OTC CCP | AID020 | **5** | **2xR3, 1xR1**  Avoided from 2020-2021. New risk in 2024 just R1 | | F7 | AID181 | **5** | **2xR3, 4xR2**  Continuously avoided/reassessed since 2020. Currently accepted risk in 2024 is rated R2 | | Corporate IT Active Directory | AID415 | **5** | **6xR2**  Continuously avoided/reassessed since 2020. Current R2 risk from 2024 is overdue since 21 days (24.06.2025) | | StatistiX | AID019 | **4** | **4xR2, 3xR1**  Continuously avoided/reassessed since 2021. Currently accepted risk in 2024 is rated R1 | | T7-Nodal | AID364 | **4** | **3xR2**  Continuously avoided/reassessed since 2021, with a gap in 2022. Currently accepted risk in 2024 is rated R2 | | BluePrism | AID425 | **4** | **1xR3, 3xR2**  Continuously avoided/reassessed since 2021. Repetitive issue not resolved. Ongoing risk treatment from 2024 is rated R2 | | Swift Connectivity | AID512 | **4** | **3xR2, 1xR1**  Continuously avoided/reassessed since 2021, with a gap in 2022. Currently being reassessed in 2025. | | AST Monitoring | AID543 | **4** | **5xR1**  Continuously avoided/reassessed since 2021, Latest risk from 2024 is overdue since 24 days and rated R1 (24.06.2025) | | Enterprise Service Bus (ESB) | AID562 | **4** | **1xR3, 2xR1**  Continuously avoided/reassessed since 2023, Latest risk from 2024 is rated R1 | | SOFiE | AID647 | **4** | **4xR1**  Continuously avoided/reassessed since 2021, Latest risk from 2024 is rated R1 | | Telephone PBX System (Alcatel-Lucent) | AID670 | **4** | **4xR2**  Continuously avoided/reassessed since 2021, Latest risk from 2024 is rated R2 | | Mendix | AID735 | **4** | **4xR2**  Continuously avoided/reassessed since 2021, Latest risk from 2024 is rated R2 | | TPFM Platform | AID776 | **4** | **8xR2, 1xR1**  Unusually high count due to 2 major issues that have been continuously avoided reassessed since 2021. Risks are rated as R2. | | PKI Clearstream | AID1066 | **3** | **1xR2, 2xR1** | | Spot Markets Settlement System (SMSS) | AID531 | **3** | **1xR3, 2xR2** | | CCP Risk Management Platform | AID578 | **3** | **3xR1, 7xR2**  Unusually high count, given age | | SAP S/4HANA Swiss | AID789 | **3** | **2xR2, 1xR1** | | EMC Storage | AID938 | **3** | **1xR3, 1xR2** | | NetApp Storage | AID940 | **3** | **1xR3, 1xR2** | | KOFAX | AID948 | **3** | **1xR3, 1xR2** | | Token Authentication | AID960 | **3** | **8xR2**  Unusually high count, given age | | Security Management System (SMS) | AID968 | **3** | **8xR2**  Unusually high count, given age | | XIS1 | AID018 | **2** | 1xR2, 1xR1 | | Secure Transport | AID1000 | **2** | **3xR2** | | XEOPs LDAP | AID1057 | **2** | **3xR2, 1xR1** | | TPFM Feeflow | AID2014 | **2** | **3xR3** | | Nomination Management System (MTS.nom) | AID530 | **2** | **2xR1** | | Material Change Process | AID658 | **2** | **1xR3, 1xR2** | | Exchange | AID416 | **1** | **1xR2** | | ECC Toolbox CS | AID830 | **0** | **2xR3, 1xR2**  Newly identified risks in 2025 |   Observation: Significant carry-over of risks through constant re-assessment.  Fun Facts:   * Average age of the issues in the critical 20% are 3.225 Years. * The oldest issues are 5 years old   **3.2 All CIs mapped to an active AID and WITHOUT open ISRM Encryption Risks**  Further sampling round was done to cover Applications with potentially undiscovered encryption risks, hence the population of this sample was defined as:  “Exclude all AIDs with ongoing cryptography issues, defined as a violation of cryptography control A.10.1.1” and done via the following JQuery:  *project = ISRM AND issuetype = Risk AND "Relevant Controls" = "A.10.1.1 Policy on the use of cryptographic controls" AND "Security Domain" = "A.10 - Cryptography"*  These were then refined to a selection of 4 applications using auditor judgement, creating a biased sample of:   * 2x Critical Apps (+2 Backup\* Apps in case other cannot deliver on time)   + AID031 AM   + AID2151 CFS Portal   + AID065 NCMS/CEMT/EMC2\*   + AID022 Cascade\* * 2x Major Apps   + AID926 JEWEL   + AID017 CEF   Each application was asked to provide evidence of:   * Key Management Procedures * Data-in-Transit * Data-at-Rest * Data-in-Use     Conclusion: Big picture analysis indicated that 20% of DBG’s critical applications have active encryption-related issues/noncompliance, some risks having been repeatedly reassessed for the last 3-5 years. Detailed inspection of the individual ISRM tickets proved that all these risks were properly justified from a content perspective, and adequately managed/mitigated/accepted by risk owners from a formal perspective. No deficiencies identified, regular IT Risk process was followed with risk owner approval.  **AID031 AM (Account Master)**  Application description: Management of account master related reference data  AO: Pavlina Valentova BO: Gaelle Grzesitchak   * Key Management Procedures Excerpt from [SD\_Account Master\_AID031\_v3.0 (1) (2).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/AID031%20AM%20-%20Critical/SD_Account%20Master_AID031_v3.0%20(1)%20(2).docx?d=w2736601b43d54a3495d75665e1968822&csf=1&web=1&e=pxLKZL)     **Key Generation, Secure Key Storage, Key Monitoring & Rotation Intervals, Emergency Procedures are all done centrally by PKI Team. See TP2 for centralized testing.**   * Data-in-Transit Excerpt from [SD\_Account Master\_AID031\_v3.0 (1) (2).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/AID031%20AM%20-%20Critical/SD_Account%20Master_AID031_v3.0%20(1)%20(2).docx?d=w2736601b43d54a3495d75665e1968822&csf=1&web=1&e=pxLKZL)   **Conclusion: Not Ok. Finding raised. Encryption is done by the TIS access Support team, but a review should occur regularly. SD states “at least once a year” but no evidence has been provided -Refer to finding 3: Incomplete validation of implemented cryptography measures and key rotation in Account Master (AID031)**     * Data-at-Rest Excerpt from RE: IA: Cyber&IS Audit - Request for Documents (AID031 AM)  **Common source of answers for storage for local-hosted applications. - OK**   Follow-up questions:  - Verification that the TLS certificates are still valid  - SSH Keys are rotated where necessary  - TLS versions used are compliant with the guideline  - Relevant connections are still using the required TLS version  A: No definitive answer provided. No evidence of review performed as part of regular risk assessment.  Observation: No review/verification of the data-in-transit encryption state conducted prior to the performance of the regular risk assessment. IA observed a lack of established key rotation procedures for Account Master (AID031). While both issues were known to the application owner, the risks were not reflected in the application’s Risk Assessment Tool (RAT). At the time of the audit, the RAT erroneously marked control ID 188 and the associated sub-controls as fully compliant. **Refer to finding 3: Incomplete validation of implemented cryptography measures and key rotation in Account Master (AID031)**  **AID022 Cascade**  Description: CASCADE (Central Application for Settlement Clearing and Depository Expansion) Instruction Lifecycle and Settlement Engine  Volker Kresin <volker.kresin@clearstream.com>; Bernhard Bruetting <bernhard.bruetting@clearstream.com>; Yildirim Yildiz [yildirim.yildiz@clearstream.com](mailto:yildirim.yildiz@clearstream.com)   * Auditing requires in-depth analysis of the mainframe with operations colleagues. No time in audit – sidelined for backup choice.   **AID2151 CFS Portal** CFC Portal framework is a web-based platform that will be used as a single access point for underlying CFCL applications.   * Key Management Procedures Excerpt from: AIDXXX - CFS EAP Security Documentation  **Generic SD text. Lacks information on emergency procedures and forwarding of logs. Upon further interviews, responsibility is delegated to CFS IT Ops team.** * Data-in-Transit Excerpt from: [CFCPORTAL Cryptography.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/AID2151%20CFS%20Portal%20-%20Critical/CFCPORTAL%20Cryptography.xlsx?d=w7cceaf73657348c5b8b511a6a3d17edc&csf=1&web=1&e=HoSIGJ)  **Review performance OK.** * Data-at-Rest Excerpt from: RE\_ IA\_ Cyber&IS Audit - Request for Documents (AID2151 CFS Portal).msg  **Common source of answers for storage for local-hosted applications. - OK**   Follow-up questions:  Q: What types of keys are generated and maintained for CFS Portal? Can you provide an overview of the public keys?  Q: What does your key-pair rotation process entail? How often is it performed? How are delays tracked?  Q: What safeguards are in place to prevent the re-use of key pairs across systems?  Q: Are key event logs forwarded to a central repository? What kind of log-monitoring is in place? What events trigger an alarm?  Q: What is the process for handling compromised keys? Who is informed? Where are these tracked?  Conclusion: Not Ok. Finding raised. During an inspection of the CFS Portal (AID2151) application’s cryptographic key management processes, Internal Audit (IA) observed that the CFS Production Support team (PRD) was unable to provide dedicated PRD procedure documentation for certificate installation and monitoring workflows within the application’s documentation. PRD referenced a work instruction for cryptographic key management. (“*AS\_WS\_Cryptographic\_key\_management (IFS)*”). However, in the section for the installation and monitoring workflows, there were no defined procedures. After IA mentioned the gap, these procedures were proactively added into the operational documentation of CFC Portal Operational Documentation v2.1. Refer to [CFS Documentation.INR.CFCPORTAL Operational Documentation.v2.1 1.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Governance/CFS%20Documentation.INR.CFCPORTAL%20Operational%20Documentation.v2.1%201.docx?d=w691223791dde4e31a956487a9ff9613a&csf=1&web=1&e=yIUf86)    Further questions to the production support team revealed that the asset’s Security Documentation of the asset was used as a working instruction, despite SDs not corresponding to a “written rule” as defined by the overarching Written Rules Framework Guideline. Refer to finding 4: Incomplete process governance of cryptography and key management processes in CFS Portal (AID2151)    **AID065 NCMS/CEMT/EMC2**  New Collateral Management System / Credit Exposure Monitoring Tool / EMC2 exposure monitoring collateral credit  Ladislav Tomaj <ladislav.tomaj@clearstream.com>; Jean-Marc Di Cato <jean-marc.di.cato@clearstream.com>; Franck Brochier [franck.brochier@clearstream.com](mailto:franck.brochier@clearstream.com)   * Key Management Procedures Excerpt from: [Security\_Documentation\_AID065\_EMC2\_V2.5.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/AID065%20NCMS%20CEMT%20EMC2%20-%20Critical/Security_Documentation_AID065_EMC2_V2.5.docx?d=w68678b4c3feb448ba5404046cfe3a564&csf=1&web=1&e=LQtvdA)  **Handled centrally by the PKI team, see TP 2 for centralized testing – OK**  Excerpt from: RE: IA: Cyber&IS Audit - Request for Documents (AID065 NCMS/CEMT/EMC2)  **Known weakness addressed as part of AMELI, no further testing required.** * Data-in-Transit Excerpt from: RE: IA: Cyber&IS Audit - Request for Documents (AID065 NCMS/CEMT/EMC2)  **Evidence of data-in-transit - OK** * Data-at-Rest Excerpt from: RE EMC2 data at rest encryption.msg  **Common source of answers for storage for local-hosted applications. – OK** * Data-in-Use Excerpt from: RE: IA: Cyber&IS Audit - Request for Documents (AID065 NCMS/CEMT/EMC2)  **Confirmation that data in use is not in use – see initial observation**   **AID926 JEWEL** – Skipped for detailed testing due to ongoing finding 2024-067\_F11-A01  **AID797 SCILA**   * Key Management Procedures Excerpt from: RE\_ IA\_ Cyber & IS Audit - Request for Documents (AID797- SCILA)  **XEOPS is primary IT Ops partner who handles the actual management of keys. This is delegated from the asset owner with processes described in:** XEOPS Key Management 2024\_1.0\_.pdf * Key Generation * Secure Key Storage * Key Monitoring & Rotation Intervals * Emergency Procedures Document details the steps and describes them but is very high level. * Data-in-Transit   **Known gaps in data-in-transit encryption, however these are not listed in RAT. SSL Encryption is out of date** * Data-at-Rest  **Not stated in RAT** * Data-in-use  **Not in use but not needed – OK**   Follow-up questions:  Key Management:  I understand these procedures are performed by XEOPS. I’m listing the questions here for your reference but will send them to XEOPS directly.  Q: How many SSH key-pairs are maintained for SCILA? Can you provide an overview of the public keys?  Q: What key algorithm is currently in use at SCILA?    Q: What does the key-pair rotation process entail? How often is it performed? How are delays tracked?  Q: What safeguards are in place to prevent the re-use of key pairs across systems?  Q: Are key event logs forwarded to a central repository? What kind of log-monitoring is in place? What events trigger an alarm?  Q: What is the process for handling compromised keys? Who is informed? Where are these tracked?  NOTE: Plenty of answers blocked with reference to - Ongoing SKM/SKI project by Group Security (covered by Risk ISRM-149646)  Relevant project status slide taken from:  <https://deutscheboerse.sharepoint.com/teams/GO365_ItAmeliNew/Shared%20Documents/Forms/AllItems.aspx?id=%2Fteams%2FGO365%5FItAmeliNew%2FShared%20Documents%2F16%2DOrg%20Readiness%2F05%5FCommunications%20Plan%2F04%5FDeep%20Dive%20Session%20Prep%2F06%5FLanding%5FPage%5FSlide%5FCollection%2F20250701%5FIT%5FFocus%5FSession%5FIII%2Epdf&parent=%2Fteams%2FGO365%5FItAmeliNew%2FShared%20Documents%2F16%2DOrg%20Readiness%2F05%5FCommunications%20Plan%2F04%5FDeep%20Dive%20Session%20Prep%2F06%5FLanding%5FPage%5FSlide%5FCollection>    **Known gaps are addressed and covered by the SKI/SKM part of AMELI. The deliverable for an inventory is still Oct 2025 – expecting further readiness not feasible at this stage.**  Observation: Known non-compliant cryptographic algorithms in use with mitigation plan for the future. No fixed deadline, based on migration to Red Hat Linux 8. Corrections to statements made within the Security documentation to be resolved in the next update. Additionally, IA noted following minor inaccuracies regarding the communication interfaces within the application’s Security Documentation:   * the type and version of cryptographic technology securing connection I-01, refer to [RE IA Cyber IS Audit - Request for Documents (AID797- SCILA).msg](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/RE%20IA%20Cyber%20%20IS%20Audit%20-%20Request%20for%20Documents%20(AID797-%20SCILA).msg?csf=1&web=1&e=G9CEFM) and page 11 in [Security\_Documentation\_ AID797\_SCILA Partner Exchange\_v2.1.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Security_Documentation_%20AID797_SCILA%20Partner%20Exchange_v2.1.docx?d=w78021ba775084430ab87db00d198a920&csf=1&web=1&e=dBWhM8) * the current status or obsolescence of connection I-04, refer to [RE IA Cyber IS Audit - Request for Documents (AID797- SCILA).msg](https://deutscheboerse.sharepoint.com/:u:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/RE%20IA%20Cyber%20%20IS%20Audit%20-%20Request%20for%20Documents%20(AID797-%20SCILA).msg?csf=1&web=1&e=G9CEFM) and page 8 in the [Security\_Documentation\_ AID797\_SCILA Partner Exchange\_v2.1.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Security_Documentation_%20AID797_SCILA%20Partner%20Exchange_v2.1.docx?d=w78021ba775084430ab87db00d198a920&csf=1&web=1&e=9VWFhB)   Note: Non-compliant week algorithms that are being used:   * diffie-hellman-group-exchange-sha1 * diffie-hellman-group14-sha1 * diffie-hellman-group14-sha256 * ssh-rsa * aes128-cbc * aes256-cbc * hmac-sha1 * hmac-sha1-etm@openssh.com * hmac-sha2-256 * hmac-sha2-512 * umac-128@openssh.com   Conclusion: Not OK. Finding raised. Internal Audit observed the use of weak, non-compliant cryptographic algorithms. These were known to the Application Owner and had been planned for decommissioning as part of a planned upgrade to RedHat Linux 8. This known weakness was not found in the application’s last performed RAT. Additionally, IA noted minor inaccuracies regarding the communication interfaces within the application’s Security Documentation.  Refer to Finding 5 Partially insufficient management and tracking of cryptography risks in SCILA (AID797)  Data-in-Transit:  For I-01, you mentioned SSL as the encryption technology; similarly, for I-05. SSL has been deprecated and has been replaced by TLS.  Q: Are there any technical limitations that prevent the usage of TLS?    Q: What version is in use? Can you provide evidence of this usage?    Q: Is this recorded and reflected in the RAT?  For I-02, the connections between the 2 dedicated SCILA firewall clusters to SCILA servers is a justifiable reason for not encrypting.  Q: Was this however reflected in the application RAT?    Data-at-Rest:  Regarding the lack of disk encryption, the performance impact is a justifiable reason for not encrypting.  Q: Similar to the above point: was this reflected in the application RAT?    **AID017 CEF**   * Key Management Procedures  Excerpt from SC\_CEF\_AID017\_v4.3.docx    **No details mentioned, supposedly due to low confidentiality requirements of transmitted data objects.**   Follow up questions:   * Q: What are their individual confidentiality levels? Please identify these and the corresponding encryption measures employed. * A: All data objects are listed as public data, hence not requiring any encryption for the outside connections. * Q: Have these been reviewed for 2025? If not, please provide evidence of all measures and their review in 2024. This was initially requested as part of our email on 06.06. – but has not been delivered yet. * A: We did not review the cryptographic measures because we do not define cryptographic measures by ourselves; these are defined by the data sources an we do not have any influence on that. Our internal data – (in rest and in use) – is not encrypted because of the low-latency requirements and also because of the public nature of the data. * **OK – no further tests required.** |  |
| **TP4** | **4.1 DE/OE: IT security operation risks**  -- Inspect the access rights granted to the application and verify the access rights are granted on a need-to-know/need-to-have basis.  -- Examination of Authorization Concept (AC)  Sources of documents – Security Documents and Authorization Concepts  AID 1064: [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Authorization%20Concept%20AID1064%20PKI-DBAG_v1.8.docx?d=wca01ee317bb74ffcad56187d48a526a0&csf=1&web=1&e=qMOOIC) and [AID1064\_Security\_Documentation\_PKI DBAG\_v1.5 (1).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/AID1064_Security_Documentation_PKI%20DBAG_v1.5%20(1).docx?d=w28dc43a18b73409a95d31205b1028e4f&csf=1&web=1&e=wdn7Xo)  AID 1065:[Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Authorization%20Concept_AID1065%20PKI%20MSCA%20v2.1.docx?d=wb073614ae14740a4a40aec065f50fcb5&csf=1&web=1&e=5Y3g2I) and [Security Documentation\_AID1065\_PKI MSCA\_V2.1 (2).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Security%20Documentation_AID1065_PKI%20MSCA_V2.1%20(2).docx?d=w5fb31ea5d7b44d95b0560b40a7796cf6&csf=1&web=1&e=rPEvFf)  AID 1066: [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Authorization%20Concept_AID1066%20PKI%20Clearstream_v1.7.docx?d=waf8632d0f0334fdb808da510cf529793&csf=1&web=1&e=0037NV) and [Security\_Documentation\_AID1066\_PKI Clearstream v.1.12.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Security_Documentation_AID1066_PKI%20Clearstream%20v.1.12.docx?d=w3c7c8f6e86b9496a869013416d74792a&csf=1&web=1&e=7x17hv)  **4.1.1 Application 1: AID1064 – PKI DBAG**  Authorisation Concept retrieved from VMT during fieldwork phase.  IA inspected the application [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Authorization%20Concept%20AID1064%20PKI-DBAG_v1.8.docx?d=wca01ee317bb74ffcad56187d48a526a0&csf=1&web=1&e=qMOOIC) and the [extract from IIQ (dated 16 June 2025)](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/IIQ%20Roles%20(16June%202025).xlsx?d=wccc4a4a145cb4f4f99cc646108d77f3e&csf=1&web=1&e=8SMxjB) and performed analysis. IA noted that the entitlements/roles were not in sync from the description in AC and the implementation in IIQ. There are 42 IT roles and entitlements existing in SailPoint IIQ but not in the Authorization Document and there are 4 IT roles and entitlements existing in the Authorization Document but not in SailPoint IIQ. Refer to [Roles and Entitlements\_AID1064.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Roles%20and%20Entitlements_AID1064.xlsx?d=w253863ad66014da9be3d00ce6c064844&csf=1&web=1&e=h1b08W)  **4.1.2 Application 2: AID1065 – PKI MSCA**  IA inspected the application [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Authorization%20Concept_AID1065%20PKI%20MSCA%20v2.1.docx?d=wb073614ae14740a4a40aec065f50fcb5&csf=1&web=1&e=5Y3g2I) and the [extract from IIQ (dated 16 June 2025)](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/IIQ%20Roles%20(16June%202025).xlsx?d=wccc4a4a145cb4f4f99cc646108d77f3e&csf=1&web=1&e=8SMxjB) and performed analysis. IA noted that the entitlements/roles were not in sync from the description in AC and the implementation in IIQ. There are 26 IT roles and entitlements existing in SailPoint IIQ but not in the Authorization Document. Refer to [Roles & Entitlements AID1065.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Roles%20%26%20Entitlements%20AID1065.xlsx?d=wf884b28a425d4d1fb9e05ba2cc3e070f&csf=1&web=1&e=cAQYj2)  Additionally, the SoD analysis was not prepared as per matrix template and implemented within IIQ.  **4.1.3 Application 3: AID1066 – PKI Clearstream**  IA inspected the application [Authorisation Concept](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Authorization%20Concept_AID1066%20PKI%20Clearstream_v1.7.docx?d=waf8632d0f0334fdb808da510cf529793&csf=1&web=1&e=0037NV) and the [extract from IIQ (dated 16 June 2025)](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/IIQ%20Roles%20(16June%202025).xlsx?d=wccc4a4a145cb4f4f99cc646108d77f3e&csf=1&web=1&e=8SMxjB) and performed analysis. IA noted that the entitlements/roles were not in sync from the description in AC and the implementation in IIQ. There are 68 IT roles and entitlements existing in SailPoint IIQ but not in the Authorization Document and 12 IT roles and entitlements existing in Authorization document but not in IIQ. Refer to [Roles & Entitlements AID1066.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Roles%20%26%20Entitlements%20AID1066.xlsx?d=w5fef30ea230e4a1f9bacd5b85b9f0384&csf=1&web=1&e=m0HOXG)  **IA was informed by Security IT - Digitise, Evolve & Innovate (U) unit that discrepancy between the IIQ roles and the entitlements are being tackled at the group level through the AMELI project, specifically within the DAC – Digitalized Authorization Concept. Under this initiative, all application owners are required to record the information from the Authorization Concept into the new DAC system, which is integrated with IIQ, ensuring that all IIQ roles are automatically captured and updated within the Authorization Concept documentation for all applications.**    **As PKI services (AID1064, AID1065, AID1066) are included as part of AMELI – DAC Wave 4 with the Due Date of the end of July 2025, IA didn’t raise a finding.**  Conclusion: Ok. No issues noted for the Close-out list.  **4.2 DE/OE: IT availability and continuity risks**  -- Obtain the Security Concept on the related IT Application and validate that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continuity.  -- Inspect the Security Concept and APMS whether RTO or RPOs are defined and in line with business needs.  -- Validate the adequacy of the Disaster Recovery Plan (if Availability=Critical)  -- Inspect relevant documentation whether any incidents occurred during the test on the applications in scope and if they were handled adequately and in time.  **4.2.1 Application 1: AID1064 – PKI DBAG**  IA inspected the supplied PKI DBAG Security Document v1.5 from December 2024. Refer to [AID1064\_Security\_Documentation\_PKI DBAG\_v1.5 (1).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/AID1064_Security_Documentation_PKI%20DBAG_v1.5%20(1).docx?d=w28dc43a18b73409a95d31205b1028e4f&csf=1&web=1&e=wdn7Xo). IA validated that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continiuity. In the Security Concept and APMS, RTO or RPOs are defined and in line with business needs. No relevant incidents occurred during the test on the application.    The DBAG PKI is an internal Certificate Authority dedicated to internal applications and servers.    Availability of information processing facilities:  RTO: RTO <= 2 hours  Part of the yearly DRP: Yes. IA reviewed the Disaster Recovery report and verified that the application was covered in the test with no incidents occurring. Refer to [IT DR Execution Report\_2024](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Test_Execution_Report_Systems_2024_FINAL%20(4).pdf?csf=1&web=1&e=5Er09Y)    Information backup:  Recovery Point Objective (RPO): 0 hour <= RPO < 1 hour  Mirroring: Synchronous mirroring is used both on the Oracle database via the Oracle DB cluster and on HSMs via HAmode.  Backup interval: Backup is ensured by the Oracle Redo Log technology at database level. All the Linux and Windows systems hosting the different infrastructure components are backed up daily with 1 year of retention.  The Virtual Machine snapshot schedule follows the 5+1 policy, meaning that each week 5 incremental backups and 1 full backup are taken.  HSMs are only backed up when new private keys are created, or existing ones are modified, as no modification can technically happen between these events.    Backup recovery test regularly (at least yearly) performed: Yes, with the Change Request 44052038).  Incident Management: Standard DBG incident management process is followed in case of an IS incident. If an incident owner detects a security breach, the CERT team must be informed immediately by calling CERT hotline (can be reached under - 3 35 55) or sending an email (cert@deutsche-boerse.com). DBAG SOC is responsible of security incident monitoring and initial escalation to the CERT if the events are detected by the use cases implemented in the SIEM applications (e.g. unauthorized login or login attempt).  The internal point of contacts and the deputies have been addressed clearly in the document in case of any security incident (access violation, ineffective security control, breach of information, human errors) and in case of CA’s private keys compromissions.  **4.2.2 Application 2: AID1065 – PKI MSCA**  IA inspected the supplied PKI MSCA Security Document v2.1 from August 2024. Refer to [Security Documentation\_AID1065\_PKI MSCA\_V2.1 (2).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Security%20Documentation_AID1065_PKI%20MSCA_V2.1%20(2).docx?d=w5fb31ea5d7b44d95b0560b40a7796cf6&csf=1&web=1&e=ErXMVg) A validated that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continuity. In the Security Concept and APMS, RTO or RPOs are defined and in line with business needs. No relevant incidents occurred during the test on the application.    The DBAG MSCA is an internal Certificate Authority dedicated to internal applications and servers.    Availability of information processing facilities:  RTO: <= 2 hours  Part of the yearly DRP: Yes. IA reviewed the Disaster Recovery report and verified that the application was covered in the test with no incidents occurring. Refer to [IT DR Execution Report\_2024](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Test_Execution_Report_Systems_2024_FINAL%20(4).pdf?csf=1&web=1&e=5Er09Y)    Information backup:  Recovery Point Objective (RPO): 0 hour <= RPO < 1 hour  Mirroring: Mirroring is not in place.  Backup interval: Application-related backup is performed every hour via Task Scheduler. The backup includes ADCS, IIS, NDES and HSM configuration. The Virtual Machine where the ADCS servers run is backed up following the Company standard backup policy.    Backup recovery test regularly (at least yearly) performed: Yes. Backup and Restore exercises take place every year.  Incident Management: Standard DBG incident management process is followed in case of an IS incident. If an incident owner detects a security breach, the CERT team must be informed immediately by calling CERT hotline (can be reached under - 3 35 55) or sending an email (cert@deutsche-boerse.com). DBAG SOC is responsible of security incident monitoring and initial escalation to the CERT for the events detected by the use cases implemented in the SIEM applications (e.g. instance unauthorized login or login attempt). An additional control has been added on the PKI Admin Active Directory Group, that contains all the users entitled to privileged access on the Microsoft AD CS, so every modification of respective AD group (user addition, modification, deletion), is immediately reported to CERT.  The internal point of contacts and the deputies have been addressed clearly in the document in case of any security incident (access violation, ineffective security control, breach of information, human errors) and in case of CA’s private keys compromissions.  **4.2.3 Application 3: AID1066 – PKI Clearstream**  IA inspected the supplied PKI DBAG Security Document v1.12 from March 2024. Refer to [Security\_Documentation\_AID1066\_PKI Clearstream v.1.12.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Security_Documentation_AID1066_PKI%20Clearstream%20v.1.12.docx?d=w3c7c8f6e86b9496a869013416d74792a&csf=1&web=1&e=u7IXbL). IA validated that dedicated controls regarding the functionality are formally defined, esp. regarding availability and continuity. In the Security Concept and APMS, RTO or RPOs are defined and in line with business needs. No relevant incidents occurred during the test on the application.    The DBAG PKI is an internal Certificate Authority dedicated to internal applications and servers.    Availability of information processing facilities:  RTO: RTO <= 2 hours  Part of the yearly DRP: Yes. IA reviewed the Disaster Recovery report and verified that the application was covered in the test with no incidents occurring. Refer to [IT DR Execution Report\_2024](https://deutscheboerse.sharepoint.com/:b:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Test_Execution_Report_Systems_2024_FINAL%20(4).pdf?csf=1&web=1&e=5Er09Y)    Information backup:  Recovery Point Objective (RPO): 0 hour <= RPO < 1 hour  Mirroring is used both on the Oracle database and on the HSMs (High Availability mode).  Backup interval: Backup is ensured by the Oracle Redo Log technology at database level. All the Linux and Windows systems hosting the different infrastructure components are backed up daily with 1 year of retention. HSMs are only backed up when new private keys are created, or existing ones are modified, as no modification can technically happen between these events.  Backup recovery test regularly (at least yearly) performed: Yes. A backup restore test exercise is performed once per year.  Incident Management: Standard DBG incident management process is followed in case of an IS incident. If an incident owner detects a security breach, the CERT team must be informed immediately by calling CERT hotline (can be reached under - 3 35 55) or sending an email (cert@deutsche-boerse.com). DBAG SOC is responsible of security incident monitoring and initial escalation to the CERT for the events detected by the use cases implemented in the SIEM applications (e.g. instance unauthorized login or login attempt). An additional control has been added on the PKI Admin Active Directory Group, that contains all the users entitled to privileged access on the Microsoft AD CS, so every modification of respective AD group (user addition, modification, deletion), is immediately reported to CERT.  The internal point of contacts and the deputies have been addressed clearly in the document in case of any security incident (access violation, ineffective security control, breach of information, human errors) and in case of CA’s private keys compromissions.  5. Inspect relevant documentation whether any incidents occurred during the test on the applications in scope and if they were handled adequately and timely.  IA obtained the list of IS incidents records for the timeframe under review (1 April 2024 – 31 March 2025) and noted that there is no incident that occurred related to sampled PKI applications. No need for further testing. Refer to [14 Incidents records 2025-045 Audit.xlsx](https://deutscheboerse.sharepoint.com/:x:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/14%20Incidents%20records%202025-045%20Audit.xlsx?d=w3c728ec859da446b8917caac77faf00b&csf=1&web=1&e=WrIwG8)  Conclusion: Ok. No issues noted for the Close-out list. |  |
| **---** | --- | **---** |

**Procedures / Criteria / documents used:**

Links

“Audit Document” Audit - Key Management.pdf

[AID1064\_Security\_Documentation\_PKI DBAG\_v1.5.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/DCM/ISO/INH%20-%20PKI/pki_edm/Documents/PKI/Audit%20documentation/Security%20Documentation/AID1064%20-%20PKI%20DBG/AID1064_Security_Documentation_PKI%20DBAG_v1.5.docx?d=w018b74bf03fc4c809055d1ae8a00d8a2&csf=1&web=1&e=09EAhW)

[Security Documentation\_AID1065\_PKI MSCA\_V2.1 (2).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/Security%20Documentation_AID1065_PKI%20MSCA_V2.1%20(2).docx?d=w5fb31ea5d7b44d95b0560b40a7796cf6&csf=1&web=1&e=ErXMVg)

[Security\_Documentation\_AID1066\_PKI Clearstream v.1.12.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Security_Documentation_AID1066_PKI%20Clearstream%20v.1.12.docx?d=w3c7c8f6e86b9496a869013416d74792a&csf=1&web=1&e=u7IXbL)

[Authorization Concept\_AID1066 PKI Clearstream\_v1.7.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Authorization%20Concept_AID1066%20PKI%20Clearstream_v1.7.docx?d=waf8632d0f0334fdb808da510cf529793&csf=1&web=1&e=TPh1a7)

[Authorization Concept AID1064 PKI-DBAG\_v1.8 (1).docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Authorization%20Concept%20AID1064%20PKI-DBAG_v1.8%20(1).docx?d=wa9a8fd835f0a4cfd8997d15445b2d989&csf=1&web=1&e=wQto11)

[Authorization Concept\_AID1065 PKI MSCA v2.1.docx](https://deutscheboerse.sharepoint.com/:w:/r/sites/sp0281/internal/2025%20Audits/2025-045%20Cyber%20and%20Information%20Security%20(DBAG,%20ECAG,%20CBF,%20CBL,%20CFCL)/06%20Fieldwork/Crypto%26PKI/PKI%20App%20Checks/Authorization%20Concept_AID1065%20PKI%20MSCA%20v2.1.docx?d=wb073614ae14740a4a40aec065f50fcb5&csf=1&web=1&e=73pnxq)

Caveat: All notes in this document do not represent a protocolary transcript or quotations of the meetings. They would provide an overview over the content of the meeting. Further the notes may be arranged according to the topics discussed and not based on the chronological course of the meeting.