ADVA product security declaration

June 2023

CONTENTS

1. Introduction 4

2. ADVA's process landscape 5

2.1. Product lifecycle management 5

2.2. Secure development lifecycle 6

3. ADVA's product security declaration 7

3.1. Product lifecycle management 7

3.2. Product security management 8

3.3. Secure development environment 8

3.4. Security techniques (including secure updates and software signing) 9

3.5. Security testing 10

3.6. Secure configuration 10

3.7. Vulnerability and issue management 11

Version: 2.0 June 2023

Validity: This framework applies to all ADVA Optical Networking SE companies and all ADVA functions worldwide

Abbreviations

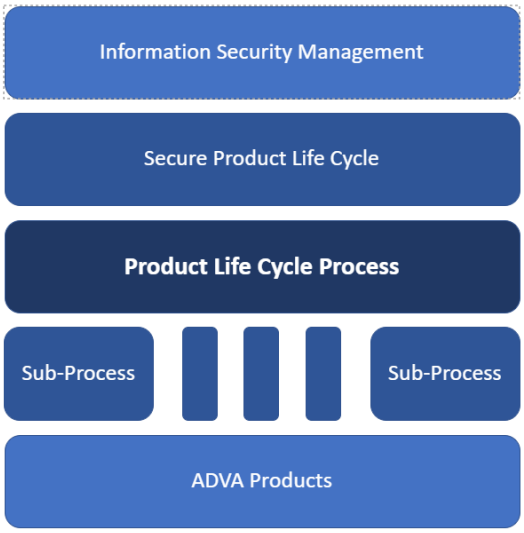
ALM = Application Lifecycle Management
ASLR = Address Space Layout Randomization
BOM = Bill of Material
CVSS = Common Vulnerability Scoring System
DSS = DevOps Signing System
DAST = Dynamic Application Security Testing
DevOps = Software Development and IT operations
FOSS = Free and Open Source Software
GA = General Availablity
HSM = Hardware Security Module
HTTPS = Hypertext Transfer Protocol Secure
KPI = Key Performance Indicator
LTS = Long Term Support
NCSC = UK's National Cyber Security Centre
NIST = National Institute of Standards and Technology
NVD = National Vulnerability Database
PLCP = ADVA's Product Lifecycle Process
PRN = ADVA's Product Retirement Notification
PSA = ADVA's Product Security Advisor
PSIRT = Product Security Incident Response Team
RCA = Root Cause Analysis
SAST = Static Application Security Testing
SCA = Software Composition Analysis
SPLC = ADVA's Secure Product Lifecycle
SSH = Secure Shell
SW = Software

1. Introduction

ADVA is a manufacturer of high-quality, robust network infrastructure for deployment in service provider and enterprise networks across the world. The security of our products is of paramount importance to us.

It is well known that telecom network infrastructure is a target of cyberattacks. A wide variety of different actors with different purposes target networks to impact availability, or steal sensitive data or intellectual property. The number and diversity of these threats is increasing, and in response ADVA must ensure the security of the products that we produce, sell or procure.

ADVA creates products according to an established product lifecycle process (PLCP) that deals with all aspects from product inception and development through to end of life. In response to the need for increased security, we are augmenting the PLCP with enhancements to specifically address security across all aspects of product development called the secure product lifecycle process (SPLC). We have also combined this with ever-more rigorous and robust IT/DevOps security practices to create a truly secure development environment.



The secure product lifecycle ensures, that ADVA products are designed, developed, tested and maintained by security-trained employees. SPLC also ensures that ADVA products are built in a secure environment and securely delivered to customers.

This document describes measures ADVA has implemented for its core products – measures that are under continuous improvement in order to support the cyber resilience of its customers and their network infrastructure.

2. ADVA's process landscape

2.1. Product lifecycle management

ADVA's product lifecycle process (PLCP) applies across all ADVA products, providing clear guidelines to successfully bring new product from concept to full deployment in target markets. PLCP is applied from concept to implementation and successful market introduction through to maintaining the mature product and ultimately to the removal of the product from the market. The lifecycle methodology is applicable to all products being realized by development projects. It explains the lifecycle and how it must be practically applied for any product being introduced, managed or withdrawn.

PLCP is a team-oriented management and delivery process applied to a cross functional organization structure following ADVA's DevOps Strategy and utilizing agile development methodologies. The PLCP establishes the concept of "key dates and phases".

Key dates are gateways between the phases. PLCP defines requirements and deliverables for moving from one phase to the next phase. A cross-functional team of people perform these activities. The SPLC phases are aligned with PLCP phases and extend requirements and deliverables defined by PLCP.

Design and development inputs involve functional and performance requirements, applicable statutory and regulatory requirements stated by customers or suppliers, or information derived from previous similar designs. Outputs from the design and development phase are verified against the requirements/inputs and are approved prior to release.

Goals of the product lifecycle process are:

- Improved planning, delivery schedules and predictability
- Reduced time-to-market for new products
- Improved product safety, security, and quality
- Improved customer satisfaction
- Increased customer involvement in product definition
- Improved revenue growth and business profitability

2.2. Secure development lifecycle

ADVA's secure product lifecycle (SPLC) ensures that modern secure practices, tooling and methodologies are followed in PLCP and ADVA's information security management system.

ADVA's Management is committed to support all aspects of Information Security related to its products, services, data, infrastructure and people.

- **... to ensure compliance with domestic and international laws.**
- **... to maintain long term competitive advantage.**
- **... to be a trusted security partner.**

All ADVA employees support the security mission.

ADVA's SPLC is a holistic process covering the complete lifecycle of the product and the entire environment in which the product is developed, maintained, tested, produced, delivered, and finally deployed in customer's facilities. Additionally, SPLC monitors all relevant product security aspects of ADVA processes and infrastructure, continuously reviewing them and defining new requirements to improve product security. It ensures that products are more secure, more resilient and fully address the security requirements of ADVA's customers. ADVA's SPLC covers product security incident response, product security certifications and independent penetration testing.

ADVA's SPLC complies with the ISO 27034-1 international standard for definitions, concepts, principles and processes involved in application security. Additionally, ADVA's SPLC ensures that ADVA's products are compliant with industry security standards and are ready for security certifications (i.e., CCC, FIPS, BSI, CSfC) and fulfil legal security regulations.

Product security improvements and mitigations are already identified in the requirement phase. Detailed product security architecture is worked out, and well documented. Approved security architecture is implemented and tested in the implementation phase. Product security verification takes part in the verification phase with products tested as they would be used by customers. In the release phase, a final security review takes place and a product security incident response plan is defined. All activities (training, requirements, features, code changes, test cases, defects) are kept in a single application lifecycle management (ALM) system.

Every ADVA product has a product security advisor (PSA), who has end-to-end responsibility for product security across all process phases and who signs off each product for production from a product security point of view. The PSA sign-off confirms that all required security activities have been undertaken according to the SPLC and that any residual risk is acceptable (open vulnerabilities, technology constraints, design compromise).

In the response phase, the PSA, leads the PSIRT team according to the product security incident response plan. They perform the security incident RCA and monitor the implementation of preventive actions. There are dedicated

backlogs for potential product security incidents. The preventive actions are stored in the defect tracking system. Both are kept and tracked in the same single ALM system.

3. ADVA's product security declaration

3.1. Product lifecycle management

ADVA's product lifecycle management is ensured by DevOps PLCP. Each product has a clearly defined lifecycle which covers well-defined conditions for product general availability, how long the product will be in general support, extended support and end-of-life dates. ADVA continues product maintenance for all products for five years after last order date. Product maintenance then discontinues unless a customer pays to extend support beyond that time. This information is distributed to our customers via product retirement notifications (PRNs).

ADVA products will only be released if they comply with this product security declaration. They are maintained through their complete lifecycle. Product maintenance includes security incident response and product security fixes. Product vulnerabilities are managed according to product security incident response plan. ADVA's security advisories and product fixes are available on ADVA's customer portal (https://advadocs.com/app/security , https://www.adva.com/en/customer-portal).

Each ADVA product has a version-controlled source code repository which logs every code modification. This audit log details the code that has been modified, added, or removed; who made the change; when the change was made; and which version of the code has been built into the released product.

Additionally, each ADVA product has a version-controlled software build (binary) repository. An audit log details which version of the product codebase has been built; when the build was made; and which binary version has been promoted to production. Build integrity is ensured by digital checksums (SHA-256). ADVA can rebuild older product versions in a near-identical fashion to their original releases.

ADVA products go through a rigorous software release cycle including security testing before a new version is released for production. Only supported tools, software components and software libraries are used within the product throughout its lifetime. ADVA utilizes professional software composition analysis (SCA) engines to manage and document all the FOSS components in the form of a FOSS bill-of-material (BOM). FOSS KPIs are established and automatically reported to company management.

Software components developed by ADVA engineers are scanned with a professional static application security testing (SAST) engine. The SAST findings are available for mandatory core review and confirmed issues then block the software change approval.

All product security incidents and product vulnerabilities are kept in a product defect log and are traceable via "vulnerability" and "incident" attributes. Defect severities of product vulnerabilities are derived from CVSSv3.1 base score, as stated in the section "Vulnerability and issue management." Beside the base score, the corresponding attack vector and link to the NVD CVE is well documented in the defect backlog. PLCP key date entry/exit criteria apply to product vulnerabilities in the same way they apply to other (functional) product defects.

ADVA maintains a single code stream for each product and multiple products are derived from the same core code base, reducing the amount of new code required for each product. There is one primary release train for each product. Forking of new versions is minimized to only when absolutely necessary and these changes are re-introduced to the main code stream at the next major release. New features are brought into the main product line during the standard development roadmap.

ADVA provides up-to-date and technically accurate product guidance for secure configuration called a secure system configuration guide. It includes very detail information on how to securely provision, manage and update the product. The secure system configuration guide is part of the product documentation suite and is available on ADVA's customer portal.

3.2. Product security management

ADVA's product security management is guarded by SPLC, which mandates a culture of security awareness within development teams. This ensures that security principles are followed. ADVA provides secure coding standards training to their staff, and the CI/CD pipelines that the build pipeline is built on ensures that these security requirements are met. Each ADVA product software codebase is maintained to a level where there is limited redundant or duplicate code. The code complexity is minimized, and software functions perform clear actions. The product software codebase has suitable and understandable comments explaining what the code is for and how it performs its actions.

ADVA's software is written in a maintainable state. Product software is well documented, and the source code is validated by professional SAST engine, reviewed, and finally approved by the software component owner. After software integration into the product codebase, intensive DAST testing takes place. Additionally, DAST testing is part of regular product regression testing, which is performed till final product release. Each shared internal component or library is kept up to date and they are supported for the lifetime of the product.

At the beginning of every release cycle SAST checkers (e.g., secure coding, overrun, string overflow, overlapping copy, buffer size, stack use, insecure function) are reviewed and approved by the PSA. The same applies to DAST tooling and the dynamic security test cases.

Insecure (unsafe) functions (e.g., strcpy(), strcat(), sprintf(), gets() …) are not allowed within ADVA's source code. Insecure functions are detected by checkers of SAST engine automatically before they enter the product codebase. However, ADVA does not prohibit insecure functions in third-party software components or in the ADVA's legacy code. Only external components that are classified as well supported (under ongoing maintenance) are used within ADVA products. The LTS versions are preferred and used wherever possible. Each FOSS component is scanned by a SCA engine for known vulnerabilities on a daily basis. Security alerts for key product security components (e.g., OpenSSL, OpenSSH, etc.) are directly monitored by the PSA and every suspicious alert is tracked as a product security incident.

ADVA's PSIRT is responsible for security incident responses as defined in the section "Vulnerability and issue management."

3.3. Secure development environment

ADVA's software build environment is simple to use, well segregated from the corporate network, not located in the public cloud, and fully protected from the internet. Only a small number of well-trained build engineers can make changes to the environment where ADVA products are developed and built. Access control is fully linked to ADVA's authentication and authorization services (LDAP), which are managed by the IT department only. The software builds and their distribution processes are fully automated and centrally orchestrated.

Only ADVA developers have access to the product codebase. Codebase access is controlled and limited. Rights to change the product codebase are controlled by the application lifecycle management engine (a developer needs an active work item to change a product codebase). Every codebase change is reviewed (minimum 4-eyes principle) and requires approval by the component owner before it enters the product codebase. ADVA does not restrict read access to product source code between product teams to control/limit redundant code in different products.

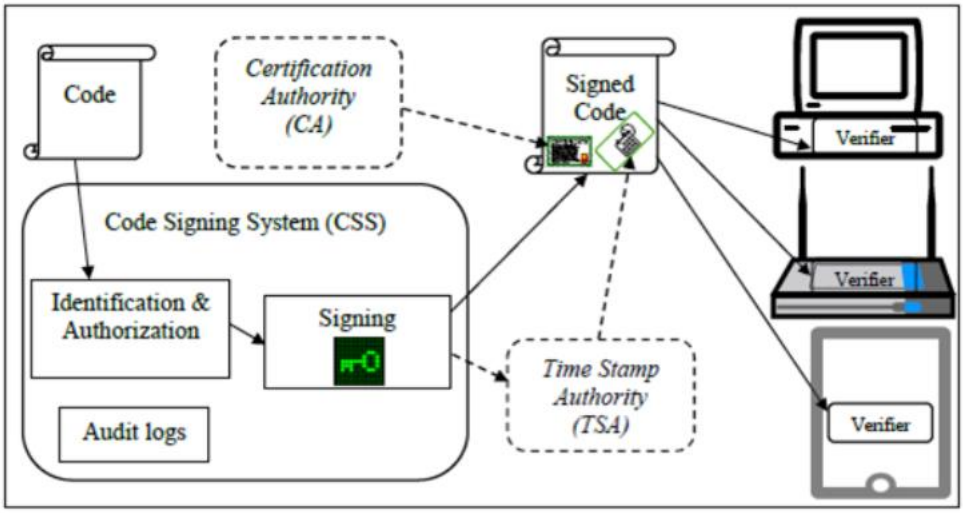
As well as source code and binary repositories, ADVA's build environment comprises:

- ALM platform ensuring product change permission and work item consistency
- SCA engine preventing usage of insecure FOSS in ADVA products
- SAST engine preventing insecure changes to the product codebase
- DSS system ensuring integrity of ADVA product binaries
- DAST engines detecting vulnerabilities in product codebase
- Fuzz engines detecting vulnerabilities in product APIs

Note: Access to very sensitive product sources (e.g., encryption) and access to very sensitive development environments (e.g., signing) is limited to necessary personnel and requires VP-level approval.

3.4. Security techniques (including secure updates and software signing)

ADVA ships executable code that has been GCC-compiled using modern software security mitigations. The stack protector (gcc -fstack-prtector) is used to stop malicious code execution in case of buffer overflow exploitation. Source fortification is enabled (gcc -D_FORTIFY_SOURCE=2) to provide additional safety checks. The binaries are generated as position-independent code to support address space layer randomization. They are linked with "-z relro, -z now" options which protects the Global Offset Table. Kernel, compiler, linker options are documented and reviewed at the beginning of every release cycle and necessary improvements are implemented. ADVA only ships Linux kernel with modern ASLR techniques enabled (randomize_va_space is enabled) for architectures that support this feature. PowerPC hardware-enforced data execution prevention is forced-on if it's the only possibility (UX and SX bits of the TLB entry control execute access to the page).



Sensitive software and firmware (e.g., encryption firmware) of ADVA is signed by ADVA's DevOps signing system (HSM integrated) in the build process. ADVA's DSS complies with NIST "Security Considerations for Code Signing". ADVA's products verify software signatures before signed binaries are installed and all time binaries are activated.

Product updates are delivered via a secure channel of ADVA's customer portal, which is hosted by Salesforce. Details about Salesforce security are available under the following link: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/misc/salesforce-security-privacy-and-architecture.pdf. ADVA's product integrity is assured by comparing hash values (SHA-256) of downloaded software versus the hash value published by ADVA on the ADVA customer portal.

Each ADVA product has a roadmap detailing when and how increased security for sensitive data processing is planned. All product security requirements are kept in a single ALM system.

3.5. Security testing

Security testing and resolution is an essential part of SPLC and PLCP to reduce vulnerabilities and the risk of their exploitation. As part of continuous integration practices, extensive tests are automatically run against ADVA products. ADVA product security features are fully tested to demonstrate correct operation according to PLCP process.

Extensive negative testing is performed against every major product release, including a wide range of potential failure cases, inappropriate message sequencing and malformed messages. Protocol fuzzing is performed against the most important external protocols (e.g., NETCONF/RESTCONF, SNMP) of ADVA products. The approach is comprehensive enough to ensure that a high proportion of code is tested.

The dynamic application security testing (DAST) engines are well integrated into ADVA's testing procedures. Selection of DAST/fuzz engines is well documented and approved for every release cycle. DAST is part of continuous regression testing, which is executed before the final product release goes into production.

Fuzzing and DAST testing is performed on products built in production mode, where all development-only features/ functions are removed, and development signatures are replaced by production signatures.

External security teams perform black box testing against selected product releases. This includes product security certifications and penetration testing. Such tests are carried out on a regular basis for FIPS and German governmental requirements.

3.6. Secure configuration

ADVA products can be easily set up to run securely. A secure system configuration guide is part of product documentation and available via ADVA's customer portal. ADVA products are pre-configured to use secure protocols by default. ADVA products do not have any undocumented protocols implemented and product backdoors do not exist.

ADVA products do not have any undocumented administrator accounts. No default passwords are left on the device after the initial set up is done properly and there are no administrative accounts hard-coded into ADVA's products.

Each ADVA product is configured to only use modern, secure protocols on the management plane. Secure protocols are used whenever possible (e.g., SSHv2 and HTTPS with TLS 1.2 default). At the request of customers, ADVA still ships products with some insecure protocols (e.g., Telnet, FTP, HTTP, SNMPv1/2, TL1). Insecure protocols are disabled by default and their activation is alarmed via dedicated standing conditions.

ADVA is explicit about the threats (e.g., password cracking, compromise of security functionality, unauthorized admin access, weak authentication endpoints) to the product that they have sought to mitigate, and those they have not (e.g., untrusted protocols).

3.7. Vulnerability and issue management

Products are most vulnerable from the point when an issue is discovered to when it is patched. Effective product vulnerability management reduces this risk. ADVA has implemented measures to reduce this risk.

ADVA has a process for issue remediation. This ensures the vulnerability is resolved in all impacted products. Vulnerabilities are patched within appropriate timeframes. This process includes root cause analysis of the issue and identifies the origin of the vulnerability.

ADVA forms cross-functional product security incident response teams (PSIRTs) being responsible for investigation and resolution of product security alerts according to product security incident response plans.

Vulnerabilities in FOSS, commercial or ADVA's components, are processed as security incidents. The ADVA severity of security incident is derived from CVSS v3.1 base score (visit https://www.first.org/) as calculated by NVD (visit https://nvd.nist.gov/). ADVA maps NVD base score into defect severity as follows:

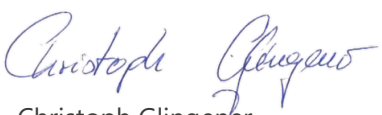
CVSS v3.1 Base Score	CVSSv3.1 Rating	ADVA Defect Severity
9.0 – 10.0	Critical	Critical
7.0 - 8.9	High	Major
4.0 – 6.9	Medium	Minor
0.1 – 3.9	Low	Minor

ADVA reserves the right to adjust, by PSIRT team, the NVD base score to reflect the real impact to ADVA products.

Normally, minor issues are not part of ADVA's security advisory and they are fixed in regular cycles of planned product releases. The PSA escalates issues to the PSIRT team that are confirmed by R&D security incidents to have severity critical or major. The PSIRT team defines deadlines for product security fixes, takes care of customer communication, records lessons learned, and works out preventive measures. ADVA keeps the product security incidents confidential until mitigation measures have been worked out and are available to ADVA's customers.

At this stage, a public announcement of potential vulnerabilities is not planned. Based on the CVSS, ADVA internally decides how our customers will be informed. This could be done by a customer service bulletin (CSB) or by direct contact, depending on the severity of the impact regarding the customer's network. The ADVA customer portal is clearly our focus to deliver such information to our customer base.

ADVA recognizes that improving security is an ongoing task and ADVA makes it clear that completely secure products do not exist. Rather it is an ever-changing and complex area where new attacks evolve, and vulnerabilities are exploited. ADVA is committed to a continuous improvement program to improve the security of our products and processes in line with industry-best practice and governmental agency guidance.



Christoph Glingener
Chief technology officer

Appendix 1

ADVA PLCP

CONTENTS

Introduction 15

Responsibility 15

Time-to-market focus 15

Customer focus 16

Product and project ownership 16

Roles and responsibilities 16

Process landscape 17

Product lifecycle process 17

PLCP process landscape 17

Deliverables 18

Key dates 19

Phase 19

Key date review meetings and review passage criteria 19

Key date authorization 19

Product line review meetings 19

Process tailoring 20

Process maintenance 20

Conclusion 20

Definitions

Portfolio management team = The portfolio management team is the project advocate and is responsible for directing a project to ensure that the benefits are achieved and that the project is viable at all times.

Product line manager (PLM) = The product line manager is the product owner. During the development phase, the PLM is a member of the project team representing the perspective of the customer.

Release project manager = The project manager is accountable for the successful preparation and day-to-day management of the project, including responsibility for communications, co-ordination and decision making between the project team members.

Introduction

ADVA has extensive experience in developing products for service providers and enterprises. This development process has been refined over many years and has become formalized in the ADVA product lifecycle process (PLCP). This detailed internal process has been defined and followed for all products for the past 15 years. This external document summarizes the principles of the PLCP to demonstrate to interested parties that ADVA has clear control over development and maintenance of all products.

The ADVA product lifecycle process (PLCP) is a team-oriented management and delivery process, which provides a clear guideline to successfully bringing a new product from concept to full deployment in the market as a mature product and ultimately to end of life.

The PLCP establishes the concept of key dates and phases. It defines requirements and deliverable at each key date for moving from one phase to the next, performed by the cross-functional team of people performing these activities. The secure product lifecycle (SPLC) phases are aligned with PLCP phases and extend requirements and deliverables defined by the PLCP.

Goals of the product lifecycle process are:

- Improved planning, delivery schedules and predictability
- Reduced time-to-market for new products
- Improved product quality and customer satisfaction
- Increased customer involvement in product definition
- Improved revenue growth and business profitability

Responsibility

It is the responsibility of ADVA's chief technology officer (CTO) to ensure that the activities described in this process are fully implemented. It is the responsibility of the process owner to ensure that this process is kept up-to-date based on inputs received from the stakeholders defined in the roles and responsibilities section and processes are adapted as the company evolves.

Time-to-market focus

To achieve customer satisfaction, it is imperative to deliver products on time. The deliverables within this lifecycle management process also capture the quality and financial elements of the project. Completing the deliverables in a controlled manner and monitoring the project progress via phase reviews enables the development of a product in a planned development time for a specific market opportunity.

- Every project has a fully accountable leader
- Empowered project teams have the project's business success as their objective
- Projects use customer-centric design; interaction with key customers from the early stages through RFFs/ MRS to lab and field trials
- Projects are measured for desired outcomes and timeframes
- Risks are appropriately managed

Customer focus

Customer and market requirements drive the design of all ADVA products. Working with lead customers and having a good understanding of the general market requirements means ADVA products are developed to meet a defined set of criteria to specifically meet customer needs. This increases customer satisfaction for both internal and external customers.

Product and project ownership

The organizational and process structure of ADVA reflects the principle of an end–to-end product responsibility of value streams comprising cross-functional teams. All disciplines required to devise, design, develop and maintain a product over its entire lifecycle are represented within the value streams. The team members are responsible for their team's activities and deliverables. Every team member should work concurrently as part of the team, not wait with their respective activities until all dependencies are completed following an agile development principle. It is the responsibility of the entire team to maintain and archive design documents, meeting minutes of design reviews and project reviews.

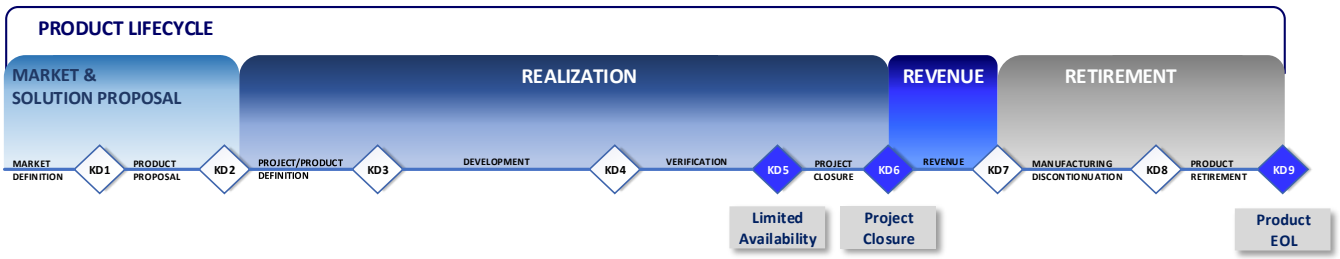
Roles and responsibilities

The PLCP and its core processes define a clear set of roles and responsibilities for all stakeholders involved in the product lifecycle processes like:

- Portfolio management team
- Product line manager (PLM)
- Release project manager
- And others

Process landscape

Product lifecycle process



The product lifecycle process covers all processes, which are needed to manage a product and product changes, starting from beginning to end of life.

It builds on the framework for various core processes, further detailing activities which need to be followed in order to achieve and maintain a mature product.

The PLCP begins with a market and solution proposal phase, where a market requirement specification is created from various feature requests and customer requirements. The phase is finalized by a KD1 review meeting.

This is followed by the realization phase, which starts with the product proposal phase and an approved business case (KD2), where a development project team is set up to continue the product lifecycle towards acceptance of the product meeting the criteria for general availability and the closure of the development project (KD6).

After closure of the development project, the product responsibility remains within the value streams. During the revenue generation phase, the PLM leads the team's responsibility to drive cost reduction activities on the product and manage any product change activities. The PLM is also responsible for setting up and managing the project team during the product retirement phase, starting with KD7 until product end of life (KD9).

During the project phases, the product or item (part of a product) status is used to reflect the maturity of a product or an item during its lifetime. Specific product maturity status needs to be demonstrated to achieve specific key dates. Overall product, and item and component statuses need to be updated as per definitions.

PLCP process landscape

The PLCP process landscape comprises a set of processes. This includes the PLCP internal standard defining the general principle, global roles and responsibilities and composition of core processes.

The core processes describe the dedicated aspects of the product lifecycle management in detail. They cover the aspects of project management, development, verification and product maintenance and governance.

The PLCP landscape consist of the following processes:

DevOps PLCP Process Landscape	Processes and Phases								
	Market & Solution Proposal	Realization					Revenue	Retirement	
DevOps PLCP Internal Standard	KD1	KD2	KD3	KD4	KD5	KD6	KD7	KD8	KD9
Secure Product Life Cycle									
Program Item Management Process									
HW Development Process									
SW Development Process									
FPGA Development Process									
System Integration Test Process									
System Verification Test Process									
New Product Introduction Process									
Component Management Process									
Product Change Control Process									
Product Transfer Process									
Waiver Process									

Deliverables

A central element of the PLCP definitions are deliverables. They serve as evidence of achieved tasks and status of the project. Deliverables may serve as input to subsequent tasks or serve reporting purposes.

The PLCP defines a superset of deliverables covering what might be required for all possible types of projects. A small set of deliverables is mandatory for all projects. The nature of projects and the products to be developed varies greatly, therefore it is the responsibility of the development team to define applicable set of deliverables needed for the given project.

The definition of deliverables covers:

- The scope – whether the deliverable covers the entire project or individual feature within the project
- The owner – who is responsible to generate the deliverable
- The reviewer – who is responsible to review and approve the deliverable
- The review criteria – against which criteria the deliverable should be reviewed
- The template – a predefined template that is to be used for generation of the deliverable
- The due date – at which key date or program status the deliverables needs to be available; this could be the final approved version or a first draft or update

Deliverables are maintained in a version-controlled system using workflow-based review and approval mechanisms.

Key dates

Key dates are milestones, which from a business perspective:

- Provide a clear and consistent decision-making process with common expectations
- Make proceed/cancel/redirect decision at critical project junctures based on clear business criteria
- Provides mechanism for management to provide funding for projects through the next phase
- Set market-based goals and execute project plans
- Ensure that customer requirements are being met
- Ensure that market requirements are being met
- Verify that product and projected market are still viable
- Confirm that product development is on schedule
- Ensure that product quality and performance criteria are being met

Phase

A phase is a period of time between two key dates where a planned set of activities must have occurred in order to satisfy the requirements for the next key date. Long-term activities might start well in advance of the given phases, but are nevertheless still justified by at least one key date.

Key date review meetings and review passage criteria

Key dates are reviewed by the portfolio management team at a key date review meeting, resulting in a decision on the future of the overall project or products/features within. A summary of the meeting results and decisions needs to be issued as minutes clearly indicating the portfolio management team decision, agreement on exceptions, any outstanding issues, impact of the issues and action plan to resolve.

Passing the review requires that the defined activities were completed, the results were delivered and acceptable according to the pass criteria by their users and the approvers, the success metrics are acceptable to the team, the product meets requirements as specified, and product and project risks are manageable.

The review status decision should be unanimous and based on the readiness criteria established by the project team at the beginning of the project. If the portfolio management team cannot reach an agreement, then an escalation procedure to higher manager should be followed. The team should make every effort to reach an agreement. Escalation should be the last resort.

Key date authorization

The composition of the portfolio management team is predefined based on the organizational and functional setup of the business units. Furthermore, the required approvals of members of the portfolio management team is defined per key date. In case members of the portfolio management team are not able to attend a key date review meeting, a deputy rule defines the appropriate substitute. Key date authorization may be achieved without conducting a meeting, if commonly agreed within the project navigation team members of the relevant key date.

Product line review meetings

The project manager reports the project status regularly during product line review meetings to the project owner. A summary of the meeting results is made available. Members of portfolio management team may participate in these meetings and/or may request the distribution of the minutes of the meeting.

Process tailoring

A project manager may tailor the PLCP process, to allow it to efficiently assure the introduction of the product and its needed quality. Project management plans or product phase-out plans should respectively document why particular activities and deliverables are not used, modified or added to meet appropriate introduction needs.

The project approach documented in these plans needs to be approved by the complete portfolio management team. This should be completed by the next key date after the tailoring has been applied. Approval for this should be included in relevant key date review meeting minutes.

If reasonable, key dates may be combined, assuming the acceptance of the portfolio management team.

Process maintenance

The PLCP is the primary means by which ADVA ensures planning, communication, coordination, and control for its new product developments and is critical to the company's continued success.

However, the process itself is only a means to an end: it is only a foundational tool to achieve its objectives. It is critical to ensure that the PLCP is maintained and continuously improved to meet the changing needs and challenges of ADVA's business.

To this end, the PLCP is subject to the following process management mechanisms:

- Process metrics
- Process improvement

This is ensured, captured and tracked by PLCP team together with quality management.

Conclusion

ADVA has extensive experience in developing products for enterprise and service provider markets. PLCP formalizes the stages of product development and support to ensure ADVA has a common framework for use for all internal development across all lines of business.

This process definition demonstrates ADVA has control over the development lifecycle, deliverables and timelines to ensure products coming to market are have appropriate feature, are built to a high standard, meet the appropriate market window and are fully maintainable until end of life.

Appendix 2

ADVA SPLC

CONTENTS

Introduction 23

Secure product lifecycle process 25

Product vulnerability management 25

Product security advisor 26

Security training phase 26

Security requirements phase 27

Security design phase 27

Secure environment design 27

Secure product design 28

Security implementation phase 28

Secure environment implementation 28

Secure product implementation 29

Security verification phase 29

Security release phase 30

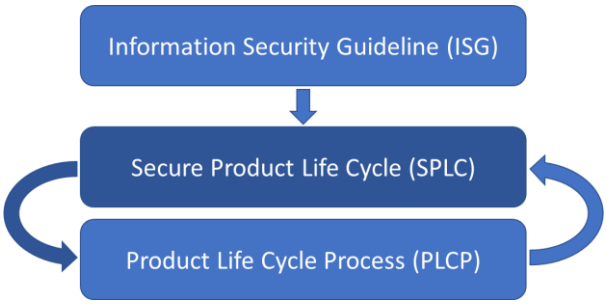
Security response phase 30

Introduction

ADVA's secure product lifecycle (SPLC) is a holistic process of bringing a new product from initial concept through to deployment of the new product in a live environment, maintenance, and support to end of life. ADVA's SPLC covers all engineering disciplines involved in product development, including the related environments and training.

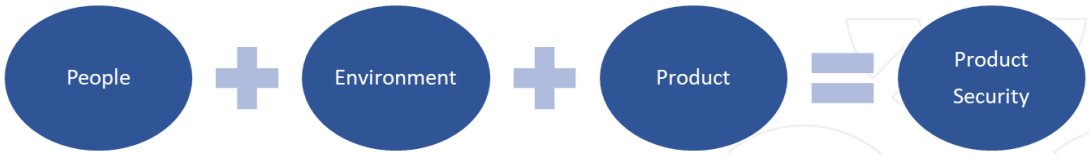
The ADVA's SPLC is an extension to ADVA's product lifecycle process (PLCP) to satisfy requirements of ADVA's information security guideline (ISG) with respect to integrity and availability of ADVA products and to the confidentiality of information processed by ADVA products. The SPLC process defines product lifecycle for all aspects of product security.

The SPLC lifecycle methodology is applicable to all ADVA products. Corporate governance defines the SPLC process as the implementation of ADVA's ISG policy within ADVA's main PLCP process.



ADVA products are developed in accordance with the main PLCP process and SPLC is an extension to PLCP, where the SPLC is focused on clear specification of information security requirements related to:

- ADVA people, performing activities on products
- ADVA environment, where product activities are performed
- ADVA products, building the infrastructure of our customers



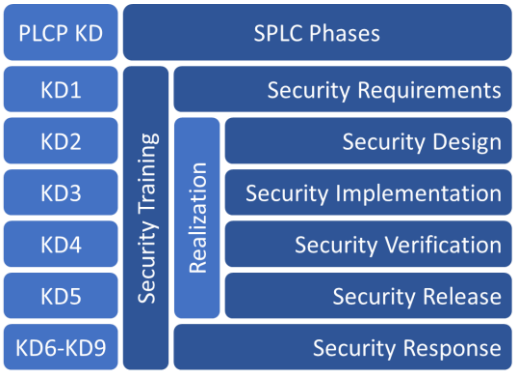
Additionally, the SPLC mandates continuous monitoring of product security status, ensures delivery of security training to the product team, and implements product security incident response.

The market, customer, regulatory (governmental, industry), and engineering security requirements define ADVA's internal standards, which together specify continuously improving product security baseline (PSBL) for ADVA products. Parts of ADVA's PSBL are publicly available to customers in the body of ADVA's product security declaration.

The SPLC process phases comply with ISO 27034-1 international standard phases to ensure high process quality and transparency to ADVA customers.

ADVA's SPLC follows the "shift left" process approach, where every security related activity needs to be executed as soon as possible to detect and correct security issues very early in the process and build a solid foundation for development of product specific features.

The "shift left" process approach is aligned with the main PLCP process via PLCP milestones, called PLCP key dates (KD). Where possible, SPLC phases are one step ahead of PLCP phases (e.g., security design takes part before product feature design starts or product development environment is ready before development begins).



Product vulnerabilities are kept together with product defects in the same database. The rating of product vulnerability is mapped into defect severity and directly impacts product quality criteria for PLCP milestones.

ADVA's SPLC activities are planned for three major areas: training, realization, and response, where the realization plan covers design, implementation, verification, and release SPLC phases.

ADVA knows that improving security is an ongoing task and ADVA recognizes that completely secure products do not exist. Rather, it is an ever-changing and complex area where new attacks evolve, and new vulnerabilities are revealed that might be exploited. ADVA is committed to a continuous improvement of ADVA's security training, product security baselines, engineering process, and vulnerability management in line with industry best practices and according to regulatory guidance.

Secure product lifecycle process

The secure product lifecycle aligns with ADVA's overall product lifecycle process, which provides a consistent DevOps methodology for product planning, design, implementation, test, release, and then on-going support.

The SPLC ensures, that ADVA products in their lifecycle are:

- Designed, developed, and maintained by security-trained employees
- Designed and developed according to legal, regulatory and customer's security requirements
- Developed, built, tested, and produced in secure environments
- Securely delivered, deployed, and placed in service
- Monitored for vulnerabilities and maintained until end of life

Product vulnerability management

Products are most vulnerable in the period between when an issue is discovered to when it is resolved, e.g., patched. ADVA's SPLC process implements measures to reduce this risk by rapidly assessing vulnerabilities and manage the response.

For each product, the SPLC requires a cross-functional product security incident management team (PSIRT), which is responsible for investigation and resolution of product security alerts according to the product security incident response plan. This plan is a mandatory security release phase deliverable.

ADVA follows the hybrid PSIRT organizational model consisting of distributed PSIRTs and a central organization coordinating cross-product security incidents.

Vulnerabilities in FOSS, commercial or ADVA's components, are processed as product security incidents. The ADVA severity of security incident is derived from CVSS v3.1 base score (visit https://www.first.org/cvss/) as calculated by NVD (visit https://nvd.nist.gov/). ADVA maps CVSS v3.1 base score into ADVA defect severity as follows:

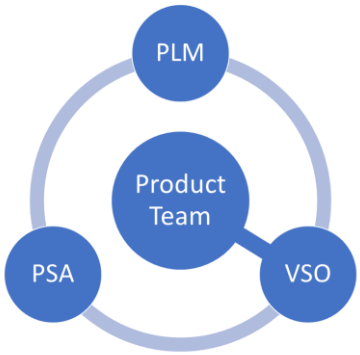
CVSS v3.1 Base Score	CVSSv3.1 Rating	ADVA Defect Severity
9.0 – 10.0	Critical	Critical
7.0 - 8.9	High	Major
4.0 – 6.9	Medium	Minor
0.1 – 3.9	Low	Minor

ADVA reserves the right to adjust, by PSIRT team, the NVD base score to reflect the real impact to ADVA products.

ADVA keeps the product security incidents confidential until mitigation measures have been worked out and are available to ADVA's customers. ADVA's security advisories and product fixes are made available on ADVA's customer portal.

Product security advisor

The product security advisor (PSA) is the most important role in the SPLC process. The PSA has end-to-end responsibility for product security across all the process phases and signs off each product release for production from a product security point of view. The PSA sign-off confirms that all required security activities have been undertaken according to the SPLC/PSBL and that any residual risk is acceptable and documented.



The PSA acts independently from the product team and is the product security partner to the product line manager (PLM) and the value stream owner (VSO), the head of product team. Together, they maintain the product security roadmap, develop PSBL, and define necessary security trainings and security backlogs for the product and for the product environment.

The VSO supports PSA by sharing with PSA product team resources as required by SPLC process, PSBL, product security roadmap, and security incident response. The PSA supports the VSO and product team by giving ad-hoc security guidance, delivering training and support.

The PSA is the main point of contact for all aspects of product security. In this context, the PSA is also the chairman of product security incident response team (PSIRT) responsible for continuous monitoring of security alerts, their immediate investigation and risk assessment. Confirmed security incidents are escalated to PSIRT and processed according to the product security incident response plan.

The PSA is the lifecycle manager for product digital certificates and product signing keys and coordinates software signing. The PSA is also responsible for complete and up-to-date evidence of all product security artefacts, their structure, and their seamless integration into product backlogs in accordance with program item management.

Security training phase

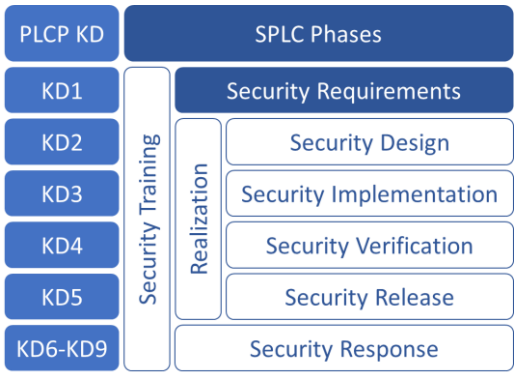
PLCP KD	SPLC Phases	
KD1	Security Training	Security Requirements
KD2	Realization	Security Design
KD3		Security Implementation
KD4		Security Verification
KD5		Security Release
KD6-KD9		Security Response

People are the most important security assets in all SPLC process phases. Design, development, testing, and operation of secure products is not possible without dedicated security training. People involved in the SPLC process need to receive appropriate and regular security training to stay informed about the continuously changing aspects of product security.

ADVA's SPLC consists of mandatory security training, which is a continuous (non-project related) process component managed directly by VSO. Evidence of security training is mandatory and maintained by HR. The PSA monitors delivery of security trainings according to the training plan on regular basis, to ensure that only security-trained personnel are working on the product.

Identification of appropriate security training for specific process roles belongs to the personal development part of ADVA's performance appraisal process.

Security requirements phase



The secure product lifecycle begins with the product security requirements phase, gathering requirements from:

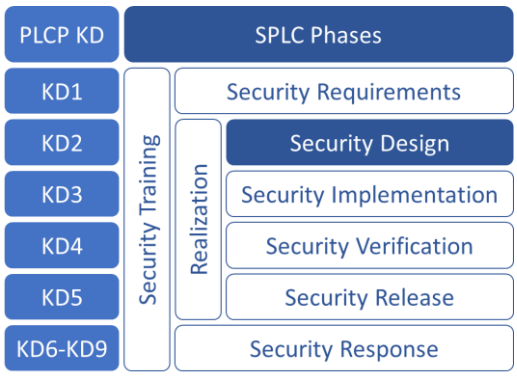
- Market and customer
- Governmental and industry
- Security certifications (CCC, FIPS ...)
- Industry engineering best practice
- ADVA internal secure engineering

Security requirements define ADVA's internal standards and together build ADVA's product security baseline for three security assurance levels (basic, substantial, and high) as stated in EU Cybersecurity Act. PSA, PLM, and VSO agree on the PSBL assurance level and PSBL scope for release project. The final agreement is the plan for security realization phases.

In the requirement phase, the PSA is informed by the PLM about the planned scope of a product release to assess the security risk associated with new product features. Product features under security risk must have additional security efforts allocated in their realization proposals.

Finally, product team resources are assigned as required by the SPLC process and agreed PSBL assurance level.

Security design phase



The security design phase consists of two dedicated design topics:

- Secure environment design
- Secure product design

Secure environment design

Overall product security strongly depends on a state-of-the-art, well-defined, and stable environment. The SPLC goal is that all changes to the environment should be applied before product realization starts.

ADVA's SPLC defines product environment very broadly. It covers people (their tasks and permissions), standards and their guidance, processes (procedures, use cases, and tasks), rules and their gates, software/hardware (their versions and configurations).

The security design phase defines the physical and digital environments ADVA puts in place to develop, produce, and deliver its products in a secure manner to guarantee product integrity and authenticity (HW, FPGA, SW, documentation, configuration) up to the deployment in customer facilities.

The environment design ends with fully completed requirements with respect to product environment, which are ready for implementation.

Secure product design

Product security depends on product architecture, which must keep the attack surface as small as possible at an architectural level and eliminate unnecessary product complexity. Product-specific attack surface and abuse cases are analyzed from a hypothetical attacker's point of view to provide developers and testers with a systematic analysis of the threat model, attacker profiles, attack vectors and assets most desired by attackers.

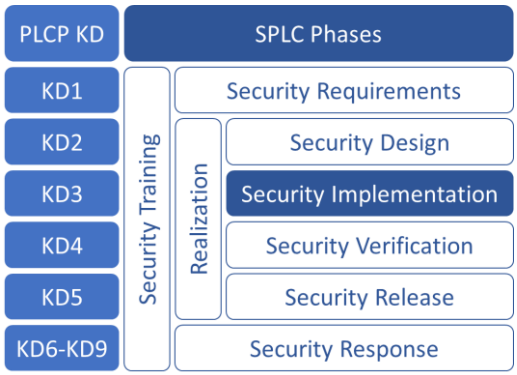
For each threat and abuse case, the product architecture risks are assessed and prioritized. Mitigation techniques for the most important risks are documented in the form of design requirements or banned components and functionality. Product hardening requirements are determined and documented.

In the product design phase, cryptographic product design takes place according to the newest recommendations of national and international authorities.

Product capability to execute security self-tests at boot-time and/or security audits at run-time should guarantee maximal test/audit coverage.

Finally, the security design of product features at particular security risk is assessed and any additional security design requirements are documented. All product security design requirements are handed over to the product team before product/feature design starts.

Security implementation phase



The security implementation phase consists of two dedicated implementation topics as well:

- Secure environment implementation
- Secure product implementation

In addition to product implementation, ADVA also implements the complete digital environment for all product-related activities. From the security perspective, the digital product environment is a service (environment as a service) which has its own security requirements.

Secure environment implementation

All the environment design requirements are implemented in the environment implementation phase before the PLCP product implementation begins.

The complete (embedded) development environment (E)DE is updated according to the security requirements. The static application security testing (SAST), software composition analysis (SCA), and dynamic application security testing (DAST) engines are integrated and configured according to the security requirements. The FOSS and third-party components are updated. Security test cases (positive) and security abuse cases (negative) are documented, automated, and integrated into the regular product regression.

The PSA ensures that the product environment is verified and released before product development starts.

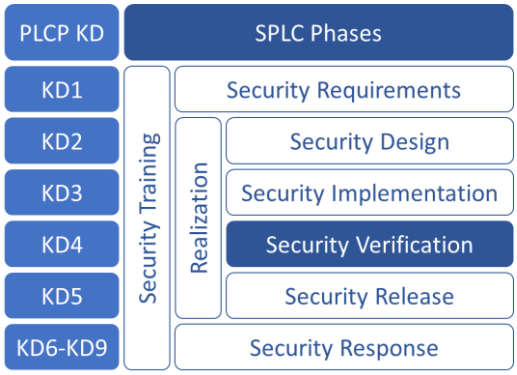
Secure product implementation

The SPLC focusses on the implementation of security design requirements into product design requirements.

The complete product security documentation is reviewed and updated to ensure that security-related documentation is up-to-date and complete before product development starts.

The PSA ensures seamless traceability of security design requirements back to the PSBL.

Security verification phase



After the PLCP security implementation" phase, SPLC deals with verification of changes applied to the product and ensures that changes to the product's secure configuration guidance are introduced as early as possible.

Security verification focuses on the product's source code, which is the main the source of security risk. Static analysis of source code is mandatory. It provides a scalable solution for the security code review and ensures that secure coding policies are being followed.

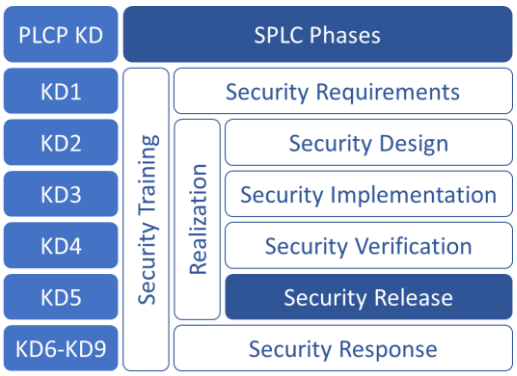
The manual code review is a mandatory part of the product source code change control. Every change to a product's source code requires change approval before integration into the product codebase. The product team must ensure that all security-relevant code (components of secure architecture) is understandable, auditable, maintainable, and testable.

Parallel to the implementation of product source code, the system security testing takes place. System security tests (DAST, fuzzing, use and abuse tests) are prepared for and executed on software built in production mode, where all debug and test functionalities are disabled or removed. Products under test must be provisioned according to the product's secure configuration guide. Additionally, penetration testing (simulated cyberattack on a product) begins with the security verification phase.

The SPLC continues with security verification tasks till the end of the security release phase.

All detected vulnerabilities must be processed as product security incidents and tracked as product defects. Product vulnerability reviews are undertaken daily. The PSA concentrates on product security status and is responsible for the mitigation of product vulnerabilities and important product security risks.

Security release phase



The security release phase it the last SPLC phase of product realization, where the focus is on:

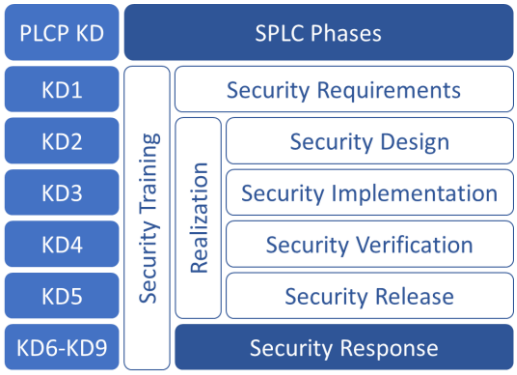
- Final review of secure configuration guide
- Preparation of release notes and list of limitations
- PSIRT team set up

The PSIRT team prepares the final version of the product security incident response plan.

The PSA is authorized to order penetration tests carried out by external authorities.

The security release phase ends with the final review of previous realization phases and PSA sign-off confirms that all required security activities have been undertaken according to the SPLC and PSBL and that any residual risk (open vulnerabilities, technology constraints, design compromise) is acceptable and documented.

Security response phase



After product release, the PSIRT team acts according to the approved product security incident response plan. The PSIRT team defines deadlines for product security fixes, takes care of customer communication, records lessons learned, and works out preventive measures.

The PSIRT team meets on a regular basis. In case of product-critical security incidents, the PSIRT team must meet immediately. PSIRT responsibility for product security ends with product end of life.

For concerns about product security, please get in touch with ADVA's PSIRT at psirt@adva.com.