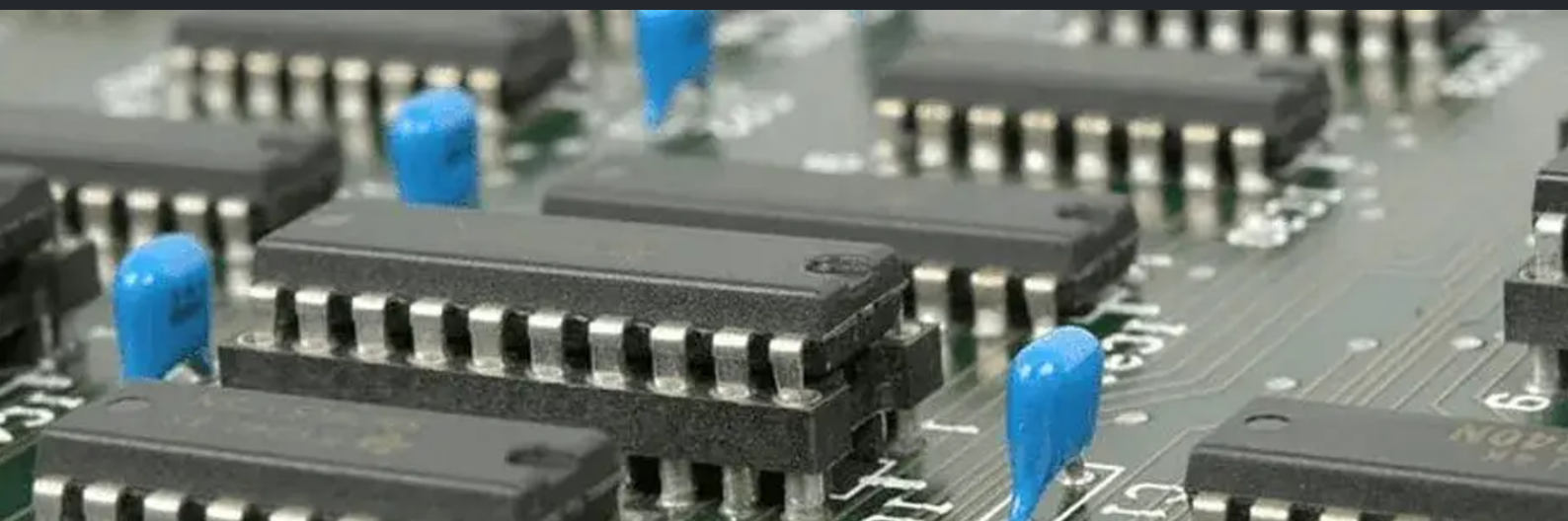


PRACTICAL GUIDE · 2026 EDITION

FSB Notification Russia and EAEU The Handbook

A comprehensive handbook for manufacturers,
exporters and product managers



FUNCTIONS · CATEGORIES · FORM · REGISTRY
TESTING · DOCUMENTATION · CHECKLISTS

How to use this handbook

Identify cryptographic functions, choose the proper route and allocate actual goods.

This handbook addresses manufacturers, exporters, importers, plant builders, product owners and technical specialists. It covers notification of cryptographic goods for Russia and the Eurasian Economic Union. The foundation comprises the AC Inorms page, regulations archive and official EAEU sources. An original working method, product examples and printable checklists supplement these foundations. German and English editions share the same structure. Explanations and templates are not official translations or decisions on an actual product.

Structure and use

Pages 4-12 explain law, goods allocation, categories and procedural routes. Pages 13-20 cover roles, records and technical particulars. Form, filing, timing and registry follow on pages 21-28. Pages 29-34 cover customs, changes and further releases. Product groups and cases appear on pages 35-41; FAQs, planning and worksheets on pages 42-47. Sources and contact details conclude the guide.

Edition 1.0 · As of 14 October 2026

Notification, EAC conformity and radio requirements are separate tasks. Wi-Fi or Bluetooth alone does not establish a universal notification duty for every product. Actual goods and functions govern.

Contents

Linked chapters and printable working aids.

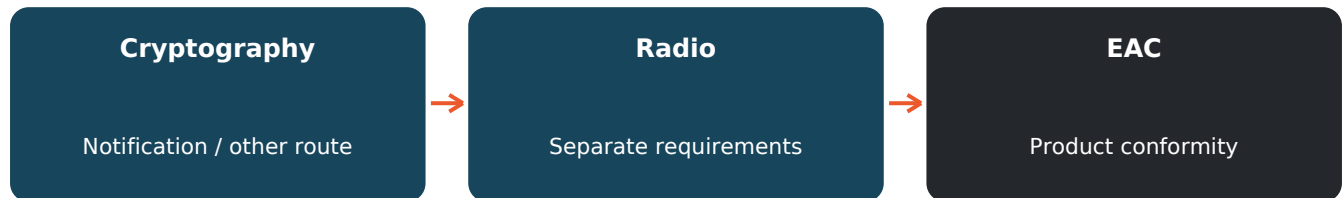
Chapter	Pages
Foundations, categories and procedural routes	4-12
Roles, inputs and technical records	13-20
Form, filing, timing and registry	21-28
Customs, changes and further releases	29-34
Product groups and cases	35-41
FAQs, planning and worksheets	42-47
Sources and contact	48-50

Suggested starting point

Record goods, models, firmware, cryptographic functions, goods code and actual customs operation. Then review existing registry coverage.

What FSB notification establishes

Registered notification of technical and cryptographic characteristics.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Content	Identity, purpose and actual cryptographic functions.
Basis	Manufacturer particulars and own technical evidence.
Authority	Competent member-state security authority.
Russia	Review registration with the competent FSB unit.
Effect	Eligible route under Annex 9 and registry entry.

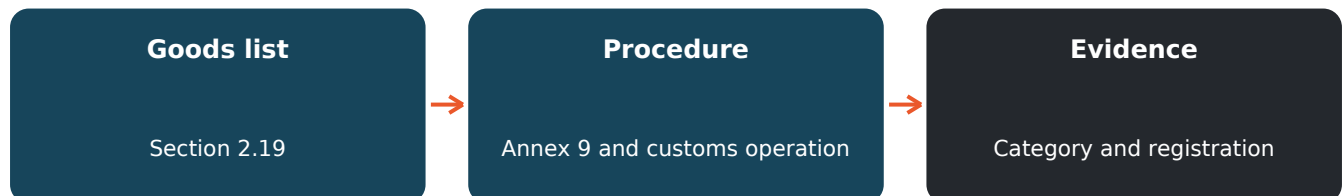
Notification does not establish electrical safety, general cybersecurity certification or overall product quality. It describes declared features under the relevant non-tariff route. FSB notification denotes the Russian authority route; the EAEU has competent member-state bodies and a common registry. Goods are covered only where actual features match. Connect technical inputs, approved notification and registry particulars in the file.

In practice

Keep notification and EAC status separate.

Legal foundations: list and procedure

Apply Decision 30/2015 in the relevant edition.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Decision 30	Non-tariff measures in third-country trade.
Section 2.19	Cryptographic goods list.
Annex 9	Import, export and associated evidence.
Sub-annexes	Registry, notification rules, form, categories and personal use.
Interfaces	Review radio goods 2.16 and specialist goods 2.17 separately.

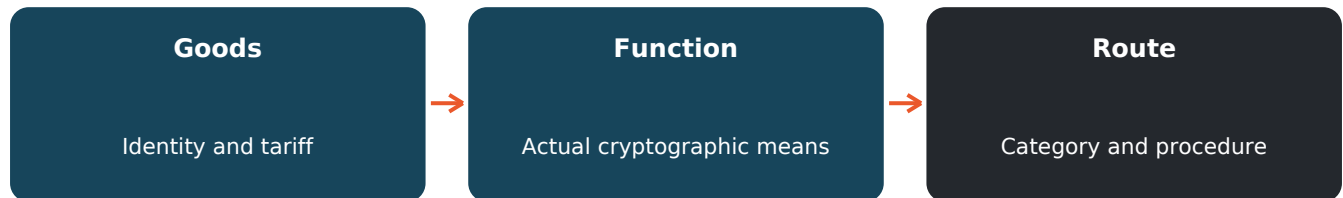
Read the 2015 framework with amendments. The official consolidated full text includes amendments through April 2026; separately provided Annex 9 incorporates in particular 165/2023 and 69/2024. Later amendments to other goods sections do not automatically alter all cryptographic provisions. Record the edition and actual clauses used. General EAC product rules do not replace non-tariff review. Retain the legal-status date in project records.

In practice

Review goods list, categories and customs procedure together.

When goods may fall within scope

Assess goods description and actual functions together.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Goods	Product description and correct tariff allocation.
Function	Encryption, signature, authentication or further means.
Component	Hardware, software, module and included systems.
Procedure	Import, export or specialist customs situation.
Outcome	Justify scope, exclusion or eligible evidence route.

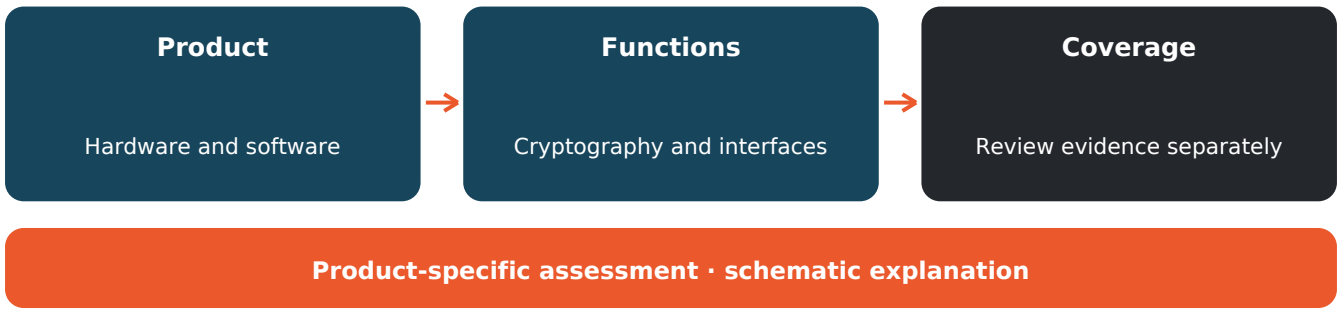
A generic name such as router or controller is insufficient. Review supplied firmware and embedded modules. Relevant functions extend beyond payload encryption under the statutory definition. An ex tariff position does not cover every product classified there. Functional characteristics constrain the goods description. Document out-of-scope decisions as traceably as in-scope findings. Unknown features are not treated as absent.

In practice

Connect hardware, software and use in one product brief.

Wi-Fi and Bluetooth: no universal answer

Radio technology prompts review rather than completing classification.



Assessment area	Project implementation
Wi-Fi	Security protocols and further networking functions.
Bluetooth	Profile, authentication and data protection.
Additional	TLS, VPN, storage or update functions.
Range	Review manufacturer specification and eligible category.
Module	Do not automatically transfer module coverage to whole goods.

The sector page describes a duty for all Wi-Fi and Bluetooth products. Project review refines that statement. Allocation follows goods lists, actual cryptographic functions, categories and procedure. Short-range radio may support a category assessment where all conditions hold. Do not overlook functions outside the radio channel. Non-radio equipment can also contain cryptography. Collect confirmed particulars for all interfaces rather than only the wireless module.

In practice

The phrase Bluetooth only does not replace a technical cryptographic inventory.

Notification categories 1-6

Orientation to sub-annex 4; review full conditions in the original.

No.	Focus / necessary distinction
1	Restricted cryptographic parameters: examine individual methods and thresholds precisely.
2	Limited authentication and electronic signature, including related key functions.
3	Operating-system components with specified user-change, installation and documentation limits.
4	Personal smartcards with specifically prescribed limited functions.
5	Specified receiving/broadcast equipment with limited encryption purpose.
6	Specified copy-protection/content-access functions without general user access.

A category is not a blanket exemption. Review each function against actually satisfied conditions. Category 1 is not a universal upper limit for modern cryptography: other categories may cover different functions. Justify selection using confirmed characteristics. This abbreviated table is insufficient as the sole classification basis.

Technical approval

Record category, function and source together in the matrix.

Notification categories 7-12

Consider functional limits and cumulative conditions.

No.	Focus / necessary distinction
7	Specifically designed and limited banking/financial use.
8	Specified civil mobile-radio goods without subscriber-to-subscriber end-to-end encryption.
9	Radio-channel encryption only; manufacturer range without amplification/relay below 400 m.
10	Protection of technological channels in information/telecommunications systems and networks.
11	Cryptographic functionality blocked by the manufacturer.
12	Other publicly available goods satisfying all prescribed sale, change, installation and documentation conditions.

Do not select category 9 using an arbitrary short measured range alone. Manufacturer conditions and radio-channel limitation matter. Category 12 conditions apply together. Online availability alone does not establish limited user changeability, eligible installation or freely available technical documentation. Categories are not chosen solely from commercial labels.

Respect boundaries

Allocate multiple cryptographic functions individually and traceably.

Notification, licence or permit

Actual operations determine eligible routes.

Allocation

Goods and functions

Route

Notification / alternative basis

Release

Procedure and registry

Product-specific assessment · schematic explanation

Assessment area	Project implementation
Notification	Review suitable category and registration.
Licence	Prescribed import/export route under Annex 9.
Permit	Conclusion/permit for specified situations.
Exception	Use only actually satisfied exclusions.
Customs operation	Regular supply, own use or special procedures.

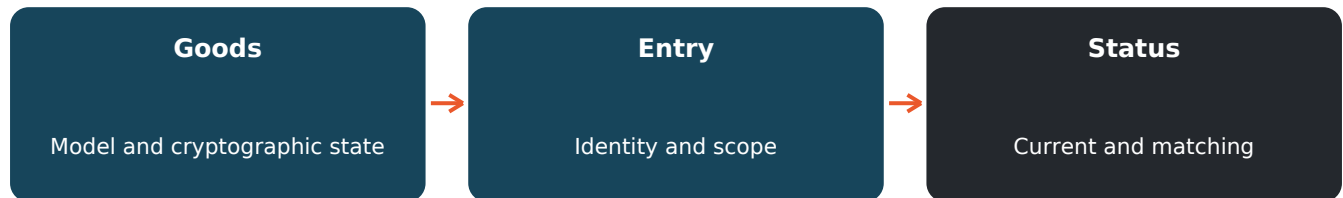
Not every covered cryptographic product qualifies for notification. Categories limit that route. Annex 9 also distinguishes ordinary supply, specified own-use cases and special customs procedures. Labels chosen by the trader do not create exclusions. Establish actual operation and goods first. If categories do not fit, resolve the competent alternative route. Keep decision, legal reference and prerequisites visible in project records.

In practice

Do not promise notification before substantiating category eligibility.

Review existing notification first

A suitable existing entry may change the project plan.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Search	Manufacturer, goods name, models and registry ID.
Status	Active, annulled or expired?
Scope	Precise goods and function allocation.
Revision	Hardware, firmware and available attachments.
Use	Confirm eligible use for actual goods.

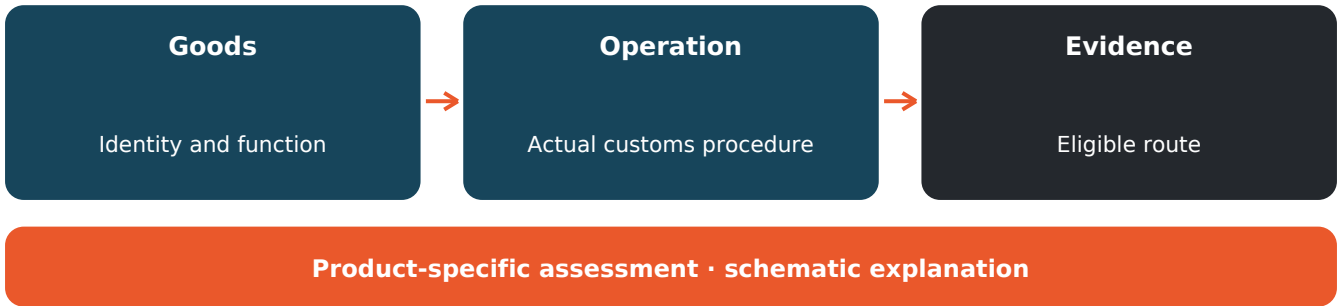
A matching brand is insufficient. Module records may differ in scope from whole equipment. Check full model names and manufacturer identity. Do not assume equivalence when detail records are absent. Distinguish filing roles from use of registered goods; changing importers alone does not decide every coverage issue. Record query date and source. Actual goods must match registered characteristics.

In practice

Confirm coverage only through complete model and function matching.

Exceptions and special operations

Distinguish personal use and commercial import.



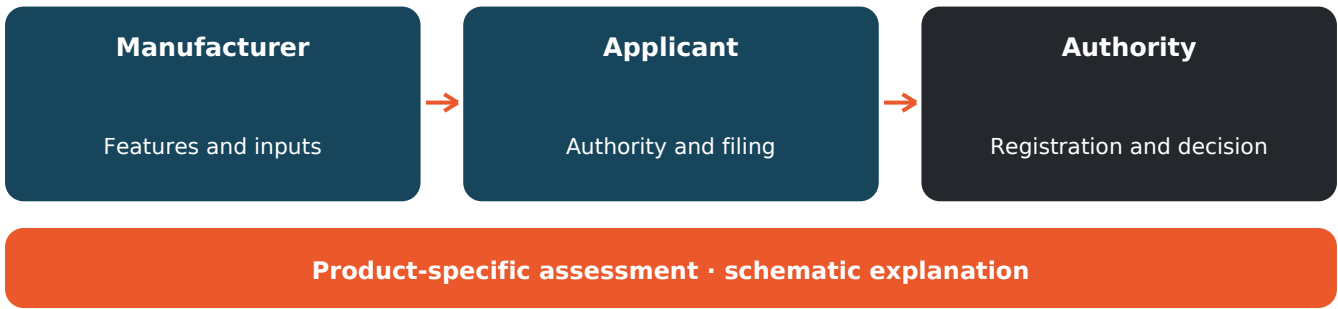
Assessment area	Project implementation
Personal	Review sub-annex 5 and actual personal use.
Own use	Conditions and prescribed evidence route.
Temporary	Plan procedure, permit and return.
Repair	Resolve reimport/reexport linkage and records.
Transit	Review actual transit movement and rules.

Personal-traveller provisions do not replace commercial shipping to customers. One unit can still be a commercial shipment. Own use does not automatically mean no documents. For repairs and temporary movements record serial identity, earlier operations and return. Transit conditions vary with the movement; the transit label alone is no blanket exemption. Confirm special situations with competent parties before shipment and record legal references.

In practice
Use special routes only for actual substantiated operations.

Manufacturer, applicant and security authority

Distinguish accountability and procedural roles precisely.



Assessment area	Project implementation
Manufacturer	Confirmed features and stable cryptographic revision.
Applicant	Manufacturer or a person authorised for this purpose.
Third country	Direct manufacturer preparation with special formalities possible.
Authority	National registration and necessary decision.
Importer	Goods allocation and intended customs use.

The sector page’s blanket claim that only an EAEU company can apply is refined. Rules provide for manufacturers or authorised persons and explicitly address third-country manufacturer organisations as applicants. Formalities still apply. Agree filing routes with the competent authority. Traders cannot independently confirm manufacturer particulars without suitable authority. Technical inputs remain allocated to the actual manufacturer.

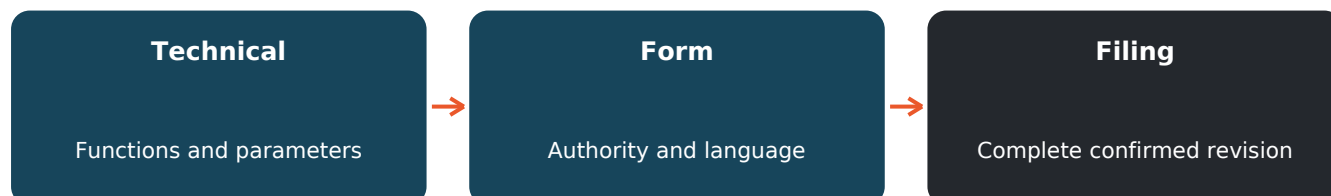
In practice

Maintain separate applicant, authorisation and customs-party fields.

Sources: [4], Unteranlage 2, Punkte 3, 19

Authorisation, certification and translation

Resolve formalities before signature and dispatch.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Scope	Identify powers to prepare and file clearly.
Identity	Manufacturer, representative and signatory.
Evidence	Date, number and eligible proof of authority.
Form	Review required certification/legalisation.
Language	Necessary certified translation and original linkage.

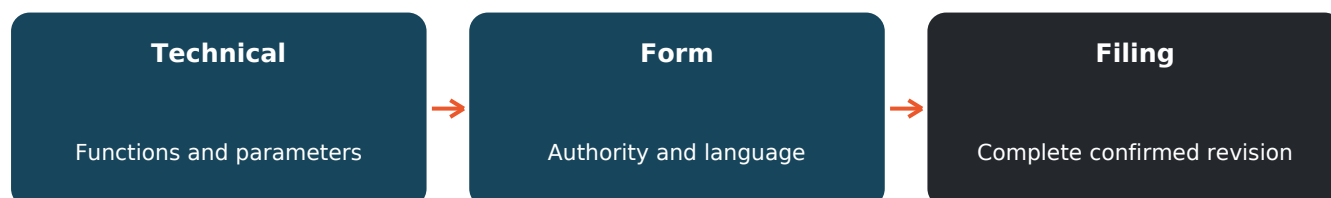
Different countries and document types do not share one universal legalisation route. Rules address certified/legalised authority documents and required translation. Direct preparation by third-country manufacturer organisations has its own legalisation duties. Check current authority acceptance before obtaining records. Scans do not automatically fulfil every original requirement. Keep names, registration particulars and addresses consistent across editions.

In practice

Do not promise a universal apostille route; confirm applicable formalities.

Technical dossier and supplementary evidence

Compile necessary inputs from reliable sources.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Product	Description, models, original names and purpose.
Cryptography	Functions, algorithms, protocols and key lengths.
Software	Firmware, versions, libraries and enabled options.
Records	Instructions, datasheet, tariff allocation and manufacturer confirmation.
Additions	CE, ISO, EAC or GOST only as relevant supplementary inputs.

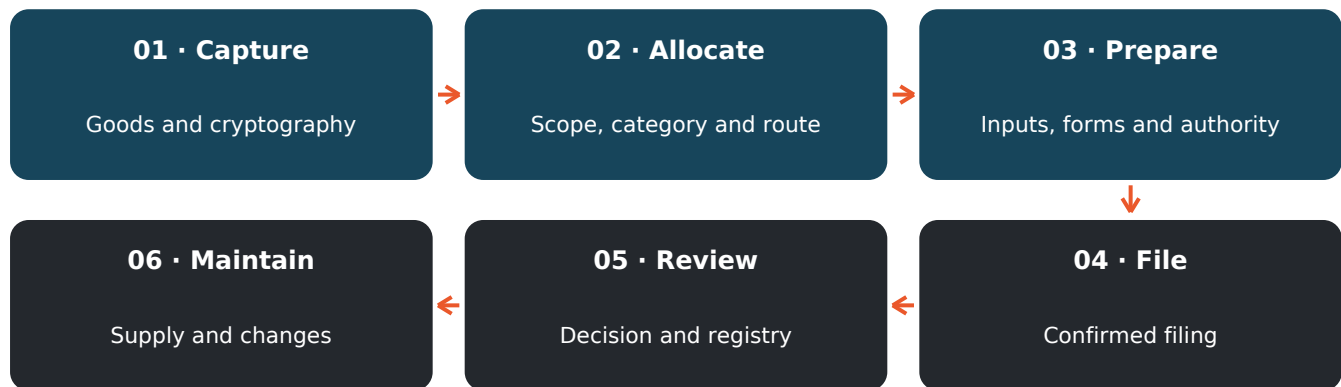
The sector page lists CE, ISO, EAC and GOST records. They are not universal prerequisites for every notification and do not replace cryptographic particulars. Agree a specific dossier list. Allocate each input to approved sources and revisions. Marketing claims of security are not algorithm evidence. Manufacturers resolve missing details. Technical approval precedes translation and filing. Secret key material is not a substitute for describing functions.

In practice

Record functions and parameters; actual private keys do not belong in general customer files.

Workflow: classification to supply release

Maintain separate technical, formal and registry gates.



Assessment area	Project implementation
01 Capture	Goods, models, functions and actual operation.
02 Decide	Category, existing coverage and route.
03 Prepare	Sources, form, authority and translation.
04 File	Complete confirmed revision to competent authority.
05 Release	Review registry, goods, customs linkage and other evidence.

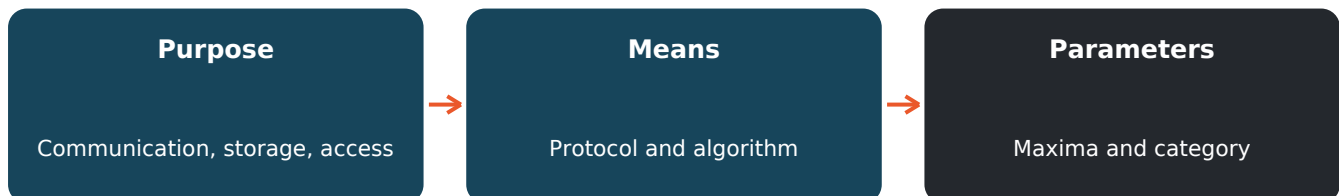
Do not begin notification planning only when goods reach the border. Library or firmware clarification may require lead time. Reconcile inputs before signature. Retain filing receipts and clarification. Connect authority registration and effective registry records traceably. Release only matching configurations. Change control then evaluates hardware and firmware evolution against declared particulars.

In practice

A signed draft is not an effective registry status.

Capture cryptographic functions completely

Review the full configuration beyond radio modules.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Transmission	Wi-Fi, Bluetooth, TLS, VPN and further interfaces.
Storage	File, disk or database functions.
Access	Authentication, signature and access protection.
Service	Remote access, updates and administrative traffic.
Components	Controller, module, library and operating system.

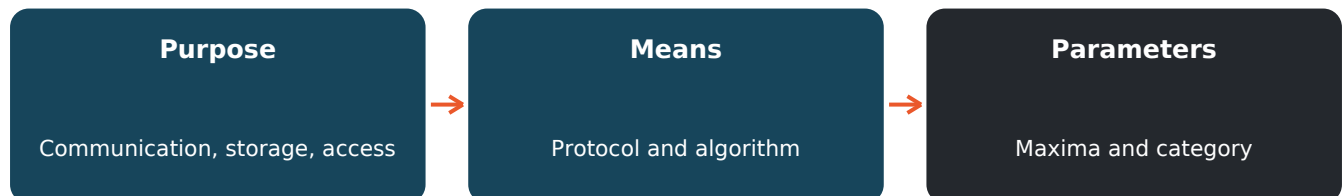
Describe the purpose of each application. Products may use several algorithms for different tasks. AES alone leaves protocols, modes and other means unclear. Review installed software and options in the supplied variant. Distinguish unused, blocked and activatable capabilities traceably. Sources may include specifications, library lists and confirmed developer inputs. Approval reviews completeness rather than entry count.

In practice

Use a row per function with purpose, source, parameters and category.

Distinguish protocol, algorithm and function

Use technical terms precisely and consistently.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Function	For example protected communication or signing.
Protocol	For example TLS with actual supported revision.
Algorithm	For example AES, RSA or ECDSA where implemented.
Hash	Distinguish hash functions and key parameters.
Evidence	Confirmed implementation rather than general standard capability.

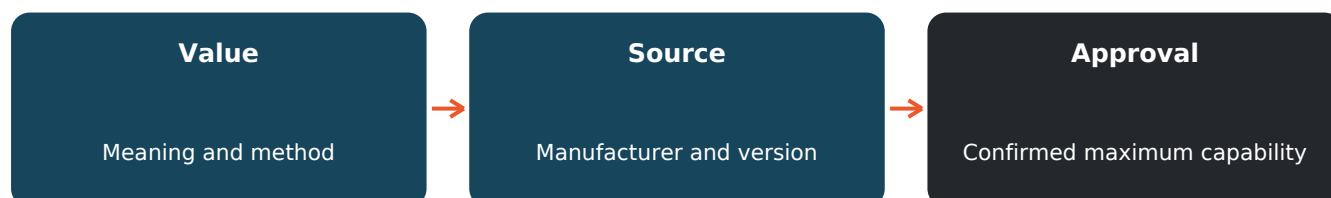
TLS is a protocol rather than one encryption algorithm. Protocols may use different means for data protection, authentication and key exchange. Describe actually supported combinations. Hash output size is not automatically a cryptographic key length. Explain functions plainly alongside precise technical names. Handbook examples are not algorithm inventories for actual products. Manufacturer approval confirms implemented capabilities.

In practice

Record protocol, algorithm and purpose in separate fields.

Key lengths and maximum capabilities

Record meaning and reference for each value.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Symmetric	Actual supported maximum key length.
Asymmetric	Method and associated parameter / key size.
Comparison	Equal bit counts do not imply equal security strength.
Configuration	Default, maximum option and manufacturer blocking.
Source	Versioned technical confirmation.

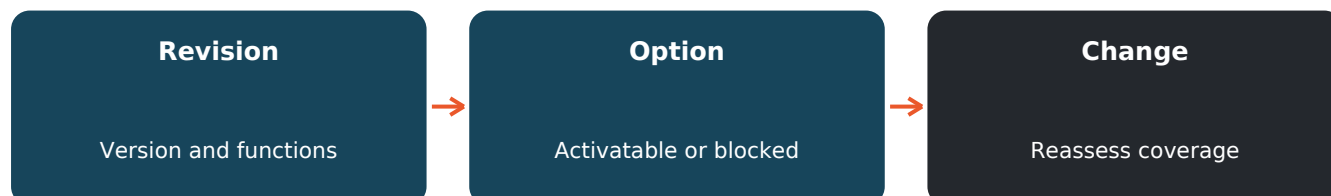
A default profile does not automatically describe maximum capability. Review activatable options and library revisions. State correct parameter bases for asymmetric methods. Do not copy hash output sizes into key-length fields. Descriptions need no actual secret keys. Confirm technical values before translation and filing. Label parameters with clear units and methods. Resolve contradictions between datasheets and firmware analysis before submission.

In practice

Describe required maximum capability rather than only current defaults.

Firmware, options and blocked functions

Keep supplied state and possible changes visible.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Version	Software, firmware and cryptography-related libraries.
Option	Licence, update, switch or configuration profile.
Blocking	Actual manufacturer measure and its conditions.
Access	User changes and service access.
Change	Assess new functions before use.

A disabled menu option is not automatically manufacturer-blocked cryptography under category 11. Confirm implementation and activation conditions. Distinguish regional and supply variants when capabilities differ. Updates may alter coverage without hardware changes. Connect approved firmware and function inventories. Substantiate unchanged claims technically. Manufacturers review relevant version changes before fresh supply.

In practice

Do not equate blocked, inactive and absent functions.

Form: goods, purpose and manufacturer

Base fields 1-3 on approved product inputs.

Name

Model and manufacturer

Configuration

Hardware, software,
cryptography

Evidence

Actual coverage

Product-specific assessment · schematic explanation

Assessment area	Project implementation
Field 1	Original names, models, brand and technical identifiers.
Software	State versions for identified software.
Field 2	Product purpose and purpose of cryptographic functions.
Field 3	Actual manufacturer and relevant contacts.
Group	Similar goods and clear individual designations.

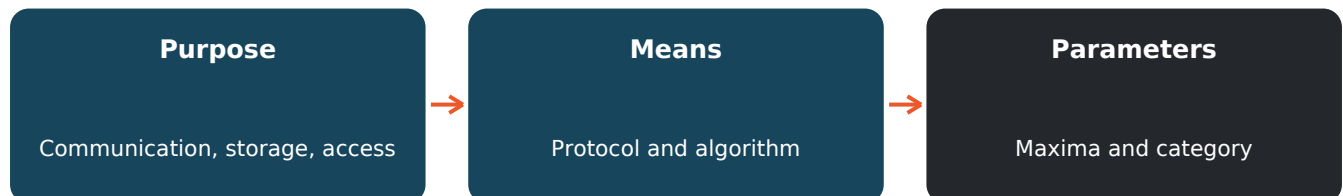
Do not translate goods names freely where doing so obscures identity. Connect commercial and technical model names. Explain intended use and the role of cryptographic functions. Identify the actual manufacturer entity. Do not group products solely because they share a brand. Review prescribed identical-means conditions. Use matching approved names in forms and goods schedules. Allocate extra pages under applicable formalities.

In practice

Reconcile form, models and datasheet before signature.

Form: cryptographic and additional functions

Complete fields 4-5 with technically aligned inputs.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Field 4	Protocols, algorithms and maximum key lengths.
Software	Name, version and implementation.
Radio	Maximum manufacturer range without amplification/relay.
Category	Function allocation under sub-annex 4.
Field 5	Prescribed undeclared-capability / special-mode particulars.

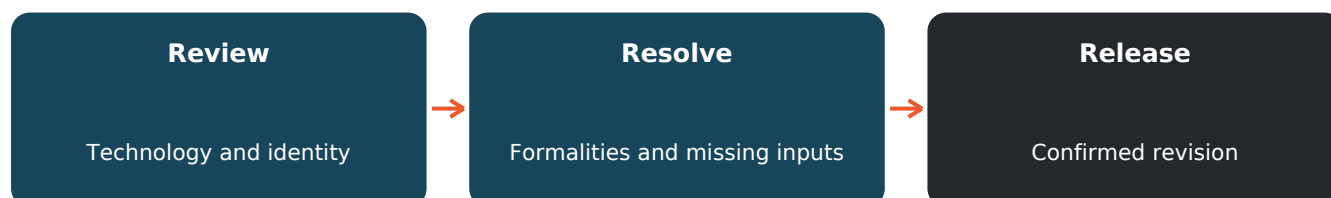
The undeclared-capability field does not invite invention of unknown features. Manufacturers technically review and confirm prescribed statements. Describe protocol and algorithm for each function. Generic privacy claims do not replace technical explanations. Trace manufacturer blocks and relevant range statements. Protocol names alone do not establish categories. Keep incomplete inputs unresolved pending clarification.

In practice

Do not record unknown features as absent without review.

Form: period, applicant and signature

Connect fields 6-9 to accountability and formal evidence.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Field 6	End date for guaranteed unchanged cryptographic functions.
Field 7	Applicant and authorised person with necessary particulars.
Field 8	Date and ID of authority documents where required.
Field 9	Preparation date in the prescribed format.
Approval	Responsible signature, name and seal where present.

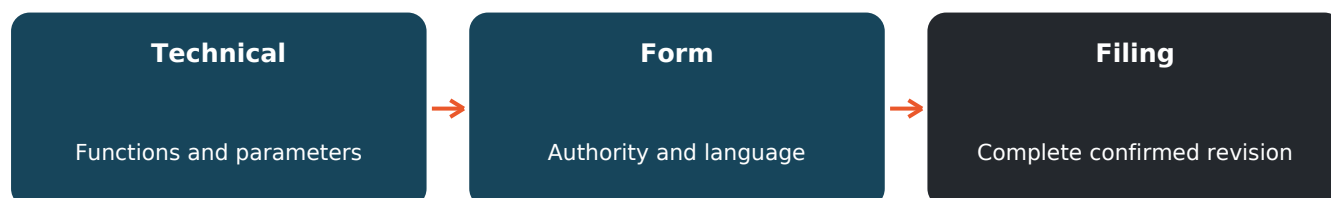
Do not derive validity from an assumed universal three- or five-year rule. Connect the period to manufacturer commitments on unchanged functions. Signatories need appropriate authority. Reconcile entity and personal particulars against evidence. Keep annex linkage and approval clear. Digital working copies are not automatically eligible authority editions. Agree format and filing route before signature.

In practice

Match duration commitments and technical version planning.

Filing: paper, files and formal records

Confirm currently accepted authority routes.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Paper	Required copies and complete annexes.
Files	Form/data structure, identifier and consistency.
Authority	Authorisation, necessary form and translation.
Electronic	Only under applicable national conditions.
Receipt	Retain date, recipient and complete filed revision.

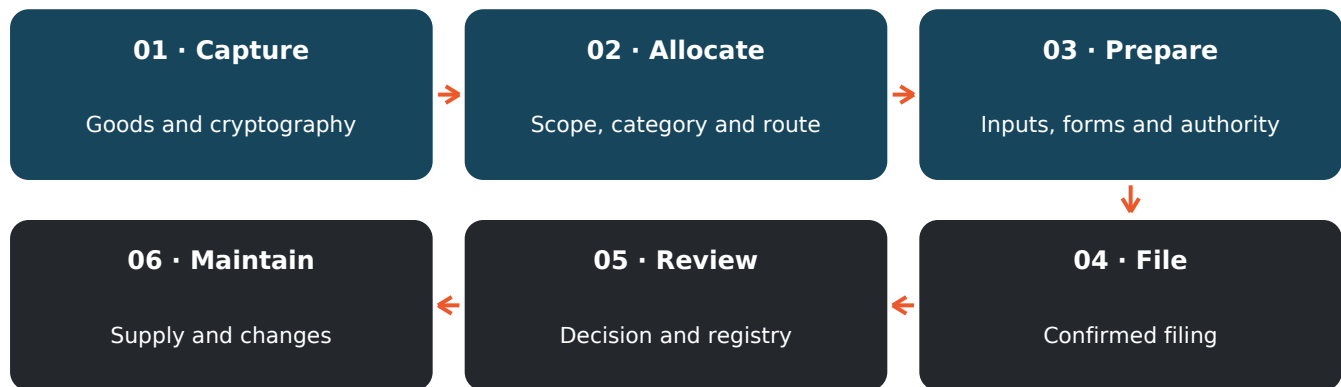
The reviewed provisions specify two copies, electronic data and authority evidence. Electronic filing is possible under prescribed national conditions. This does not mean every emailed PDF suffices. Check actual authority acceptance. Technical matrices and form content must agree. Preserve receipt and clarification. Date and identify later supplements.

In practice

Resolve filing formats before obtaining original documents.

Timing: authority phase and project duration

Distinguish procedural periods and overall scheduling.



Stage	Reviewed rule / planning
Registration or refusal	Within 7 working days from filing under paragraph 21.
EEC publication	Within 3 working days from receipt of registered information.
Combined procedural period	No more than 10 working days from filing under paragraph 23.
Pre-registration amendment	Period restarts on amendment under paragraph 26.
Overall project	Technical inputs, authority, translation, clarification and logistics additionally.

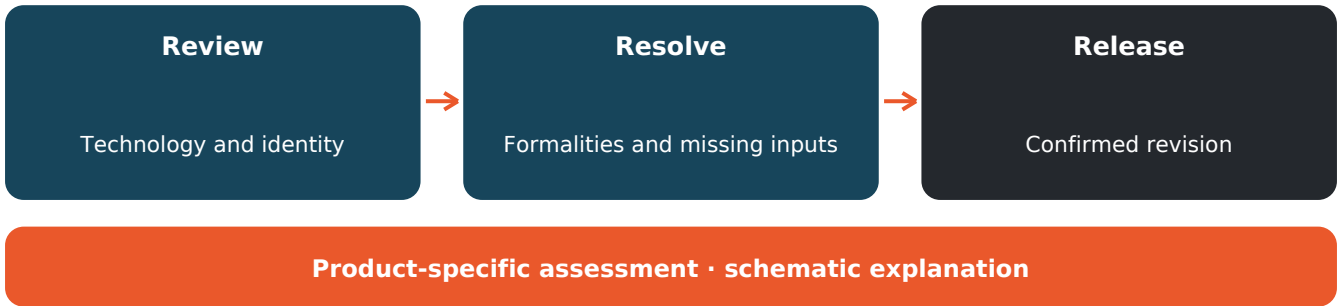
The sector page's average of 20-30 working days is treated as overall provider planning rather than statutory registration timing. Define which complete inputs start quotations. Clarification, changes and formalities may affect preparation and progress. Registry inclusion is decisive for effect.

Scheduling

Align delivery dates with technical approval and actual registry status.

Authority review and clarification

Registration is not universal laboratory certification.



Assessment area	Project implementation
Review subject	Particulars, records and procedural prerequisites.
Clarification	Affected field, source and necessary explanation.
Technical	Manufacturer confirms functions and parameters.
Amendment	Record fresh revision and timing consequences.
Closure	Retain decision and registry linkage traceably.

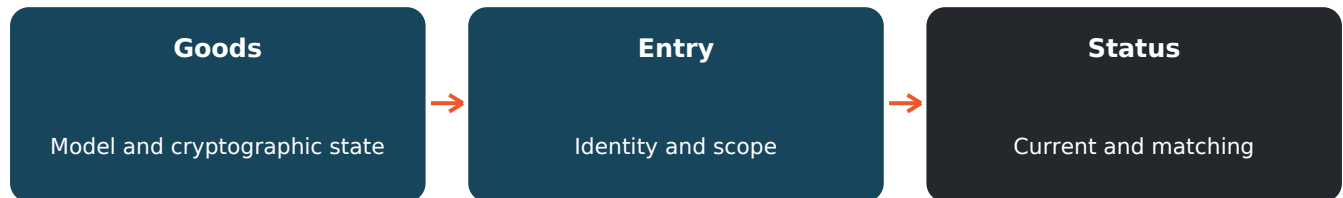
The sector page mentions document and product review. This does not establish identical mandatory laboratory tests for every notification. Necessary clarification follows the actual case and competent authority. Technical answers derive from confirmed manufacturer sources. Do not disguise contradictions through wording. Changed algorithm values may alter category decisions. Preserve editions and actual response receipts. Release includes the final submitted revision.

In practice

Track clarification with source, owner and closure evidence.

Registry review: model and status

Confirm complete coverage before supply.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Identity	Unique notification ID and source.
Manufacturer	Reconcile legal entity and address.
Goods	Models, designations and any annexes.
Period	Publication, expiry and current status.
Technical	Review supplied functions against declared inputs.

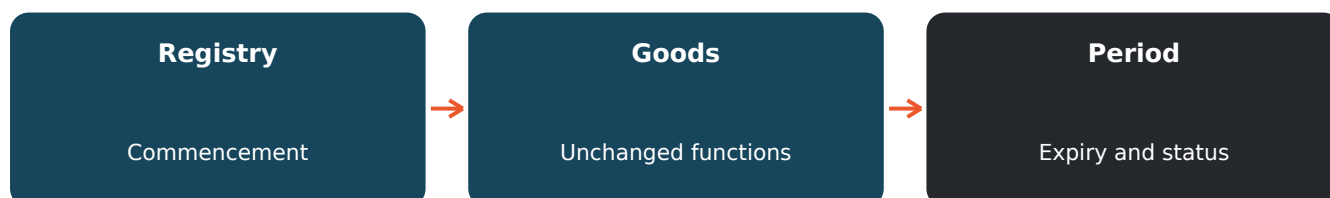
The EEC links to the common notification registry. Its content was unavailable during research, so this guide confirms no actual product ID. Project checks must preserve current actual records. Third-party portals may aid searching without replacing official source review. Match goods configuration to entries and date checks before shipping. Missing details remain unresolved until records or competent parties clarify them.

In practice

Do not copy example IDs as actual registrations into customer records.

Commencement, expiry and scope of use

Connect duration and unchanged cryptographic functions.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Start	Effective from registry inclusion of registration information.
End	Respect declared expiry and annulment.
Commitment	Manufacturer confirms unchanged functions over the period.
Scope	Identified goods and confirmed technical coverage.
Renewal	Assess changed revisions or further periods early.

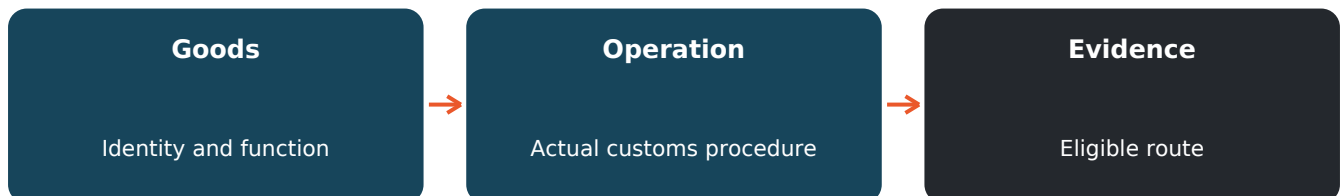
Notifications are not automatically indefinite or universally valid for five years. Review registry status and expiry. An unexpired record does not cover arbitrary new firmware functions. Align manufacturer commitments and product development. Check use of existing records against actual goods and operation. Reassess supply on expiry or annulment. Retain earlier records historically without presenting them as current status.

In practice

Time validity and technical suitability are separate release criteria.

Customs records and goods identity

Connect notifications to actual supply line items.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Goods list	Model, article, quantity and actual manufacturer.
Tariff	Correct tariff allocation and functional scope.
Evidence	Notification or prescribed alternative route.
Status	Current registry and release status before dispatch.
Records	Invoice, packing list, description and necessary schedules.

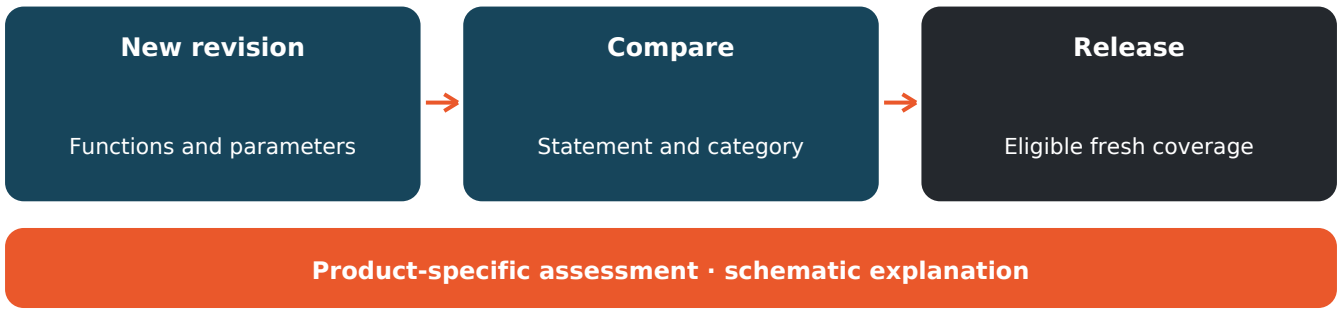
Customs descriptions and product records identify matching configurations. Shortened trade names must preserve model allocation. Plant shipments need a schedule of cryptography-related items. Do not simply attach evidence for another variant. Responsible customs parties review actual evidence routes and required references. Recheck release after last-minute substitution. Keep technical and commercial records consistent.

In practice

Each relevant line item needs a traceable coverage decision.

Firmware updates and new variants

Review cryptographic changes before fresh use.



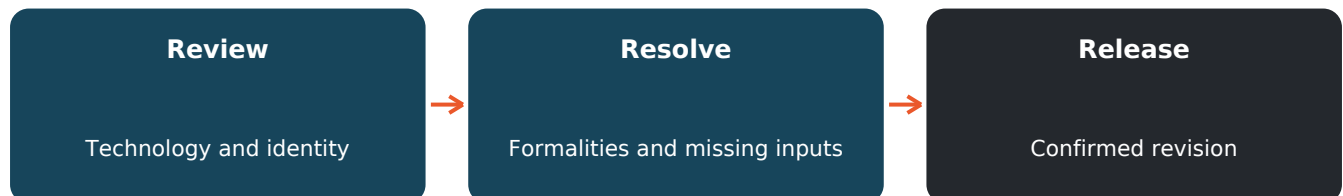
Assessment area	Project implementation
Trigger	Algorithm, length, protocol, activation or software.
Compare	Earlier and proposed function scope.
Category	Do eligibility conditions still hold?
Registry	Review current goods and function coverage.
Action	Resolve competent fresh or amended procedure.

Higher version numbers do not automatically require new notification; actual changes and coverage matter. Conversely, small patches may activate new cryptography. Record changes in a technical matrix. Do not treat new model names as identical goods without review. Authorities may annul records where functions are undeclared or parameters differ. Release therefore considers confirmed configuration, existing entries and necessary procedural consequences.

In practice
Approve consequences before distributing updates or fresh goods.

Refusal, annulment and data correction

Correct errors traceably and respect status consequences.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Refusal	Formal or content requirements unsatisfied.
Annulment	Incorrect/incomplete particulars or differing functions.
Correction	Source, affected fields and fresh edition.
Supply	Do not present unresolved or ended status as valid.
Closure	Retain competent decision and actual registry status.

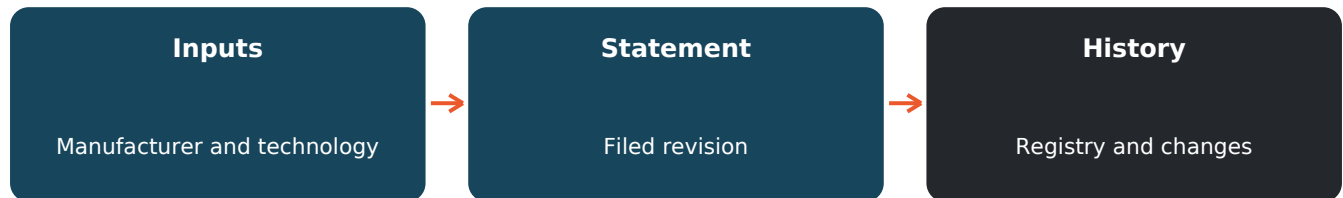
Distinguish editing from technical changes. Recipients do not independently alter registered evidence. Manufacturers clarify actual features. Paper copies do not keep ended registry status effective. Retain reasons, actions and fresh approval. Assign owners and dates to open issues. Plan new supply after necessary positive coverage decisions.

In practice

Do not confuse possession of paper records and current registry status.

Archive and technical traceability

Connect approved statements to product development.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Original	Filed edition, authority documents and manufacturer inputs.
Registry	ID, query date and status evidence.
Goods	Models, hardware, firmware and functions.
History	Clarification, changes, refusal and fresh approval.
Access	Responsible roles and reliable retention.

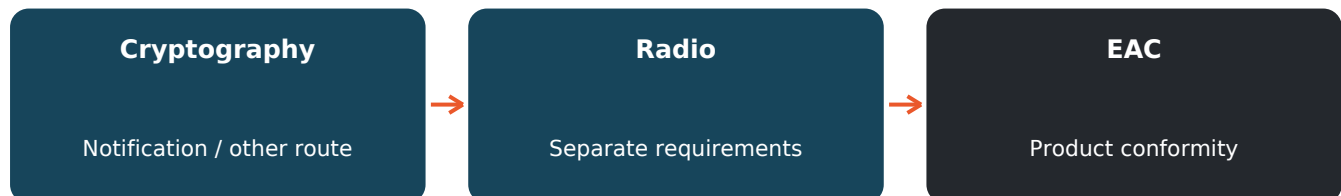
Registry IDs alone do not explain actual functions. Retain confirmed technical sources and editions. Preserve manufacturer access across provider/importer changes. Connect software changes to affected goods lists. Keep older editions traceably while removing them from current release. Periodically check status for planned supplies. New staff should be able to reconstruct original classification from records.

In practice

Store technical inputs, filed particulars and registry linkage together.

EAC, CE and other product evidence

Close cryptographic non-tariff and product-safety duties separately.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
EAC	Applicable product TRs and conformity form.
CE	European records as technical inputs.
ISO	Management evidence, not a cryptographic inventory.
GOST	Review actual national procedure separately.
Linkage	Matching goods configurations across evidence files.

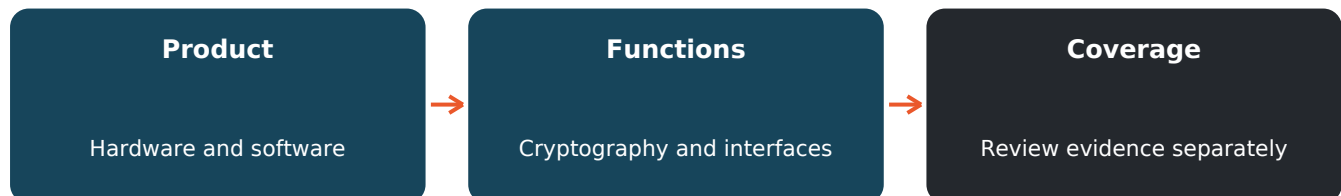
EAC declarations do not automatically satisfy notification duties. Registered cryptographic statements do not establish electrical safety or EMC. Assess low voltage, EMC and substance duties against actual goods scope. Other regulations may apply by function. A shared goods list connects separate decisions. Completed EAC status must not conceal unresolved cryptographic allocation. Use CE and ISO records only for their actual statements.

In practice

Maintain separate status and accountability for notification and product safety.

Radio requirements and other trade duties

Several legal fields can affect the same equipment.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Cryptography	Section 2.19 and Annex 9.
Radio	Section 2.16 and relevant import route.
Specialist	Special goods and national prerequisites.
Export	Review origin/export-country law separately.
Supply	Connect destination, goods, end use and operation.

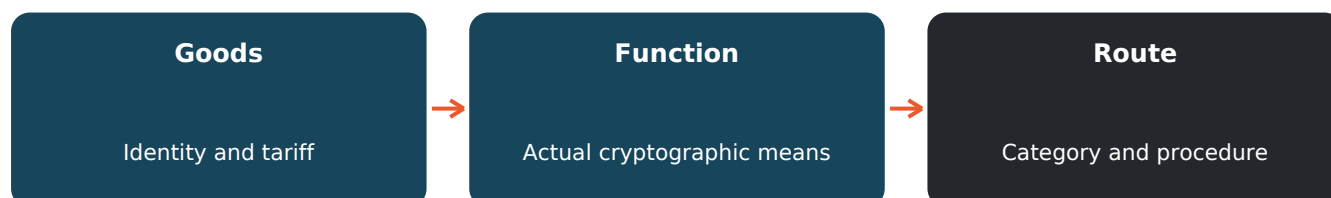
Notification does not replace radio evidence. Annex 9 refers embedded radio means to additional rules. Import eligibility does not replace export authorisation at origin. European cryptographic goods require separate relevant trade review; this handbook decides no actual permitted export. Align necessary releases before contractual and delivery commitments. All decisions concern matching configurations.

In practice

Keep import, export, radio and EAC release decisions distinct.

Computers, servers, storage and office equipment

Capture hardware and installed software together.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Computers	PCs, laptops, tablets, handhelds and servers.
Storage	Disk, file and storage-controller functions.
Office goods	Printers, copiers, fax and electronic modules.
Software	Operating system, communication and installed applications.
Coverage	Model, revision and actual functions.

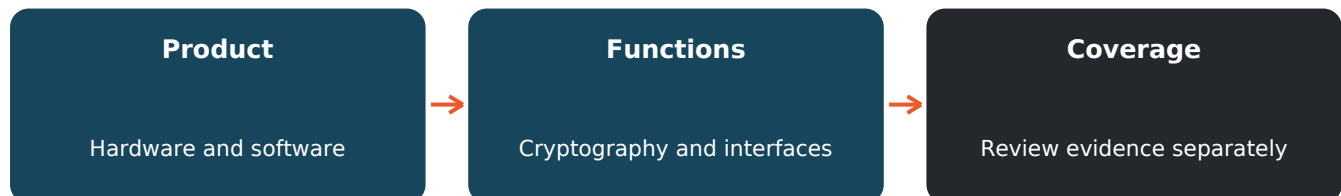
The sector page identifies these goods as typical review triggers. Categories do not create identical duties for all models. Servers may differ cryptographically from similar-looking computers. Printers can include communications or storage functions. Describe installed applications and management interfaces. Computing power alone is not evidence of cryptography. Manufacturers confirm exported options. Review existing records against actual configuration.

In practice

Do not treat operating systems and firmware as incidental sales data.

Communications, radio and entertainment goods

Allocate cryptography by interface and purpose.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Networks	Routers, base stations, communications modules and gateways.
Mobile	Phones, smartphones and civil mobile-radio goods.
Peripherals	Wireless keyboards, mice, accessories and remote controls.
Media	TV, radio, recording, playback and content access.
Special radio	Navigation and specialist frequency/radio functions.

Distinguish radio-channel protection, general network tunnels and protected-content access. These purposes may involve different categories. Smartphones may combine functions. Do not apply category 8 without reviewing all features. Confirm wireless peripheral range and protocols. Entertainment goods may include network software. Maintain radio import duties alongside cryptographic allocation.

In practice

Actual functions matter rather than the wireless marketing label.

Software, modules, cards and specialist means

Distinguish separate goods and embedded functions.

Name

Model and manufacturer

Configuration

Hardware, software, cryptography

Evidence

Actual coverage

Product-specific assessment · schematic explanation

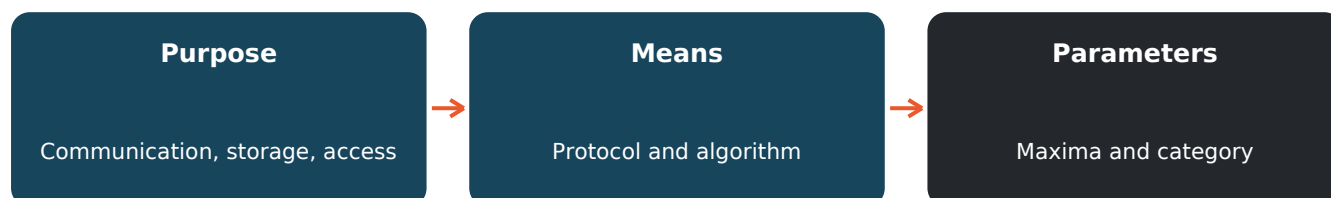
Assessment area	Project implementation
Software	Cryptographic programs and actual versions.
Modules	Electronic modules, circuits and computer parts.
Cards	Smartcards, authentication and specialist use.
Documents	Key documents and function-related media.
Specialist	Dedicated cryptographic machines or specially designed systems.

Goods lists also include software, parts and key documents. Review actual descriptions and tariff allocation. Do not automatically extend module records to new complete goods. Smartcards may have several functions needing separate review. Identify supplied software revisions; this guide does not universally equate physical import with purely electronic provision. Dedicated cryptographic means need reasoned procedural decisions.

In practice
Record software versions and separate goods identities explicitly.

Case: industrial router

Assess radio channels and additional network functions separately.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Product	Fictional router with Wi-Fi and remote service.
Function	Wireless protection plus protected network tunnel.
Inputs	Firmware inventory and confirmed parameters.
Category	Assess each function against full conditions.
Release	Model, registry and additional radio/EAC duties.

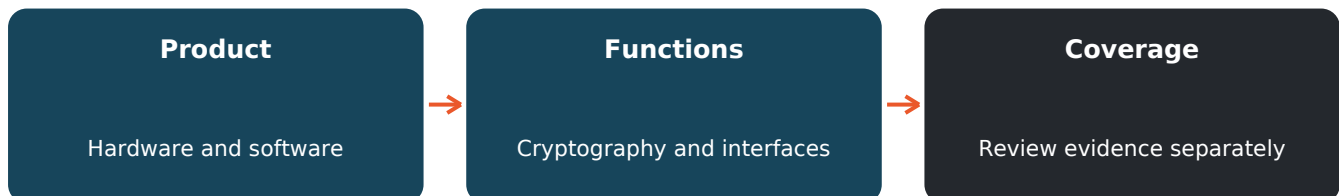
Do not assume short Wi-Fi range covers every capability. The tunnel is a separate function. Manufacturers provide protocols, algorithms, maximum lengths and versions. Justify categories for both purposes. Reconcile existing records against these inputs. Reassess added firmware features. This case promises no specific category, sample count or duration.

In practice

A function diagram prevents reviewing only the visible radio chip.

Case: control cabinet with remote service

Allocate plant components and overall goods traceably.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Supply	Fictional cabinet with industrial PC and communications module.
Inventory	Equipment, firmware, software and remote access.
Boundary	Separate module or embedded whole equipment?
Evidence	Do not transfer existing coverage without review.
Customs	Reconcile line item, manufacturer and description.

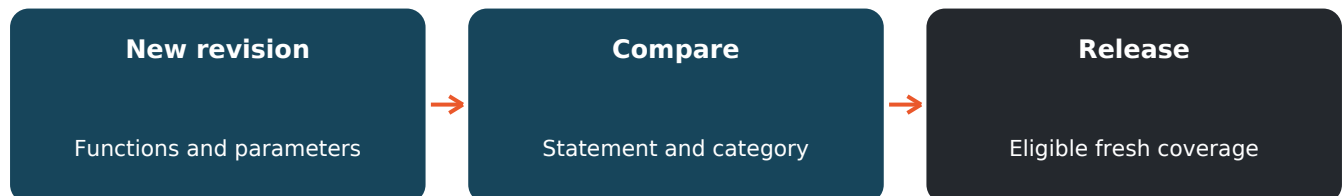
The builder receives records for several components. Create a cryptographic inventory and define actual imported goods. Known module registry IDs do not replace that decision. Industrial PCs may contain functions beyond the module. Customs parties review allocation to supplies. Machinery, electrical and radio evidence remain separate. This case creates no blanket plant notification or automatic module exemption.

In practice

Record sources and whole-goods linkage for each relevant component.

Case: software update adding capability

Review technical changes before further supply.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Earlier revision	Fictional version with documented capabilities.
Addition	Extra algorithm or activatable option.
Comparison	Reconcile maxima, purpose and categories.
Procedure	Determine competent amendment/fresh-registration route.
Release	Distribute after confirming suitable coverage.

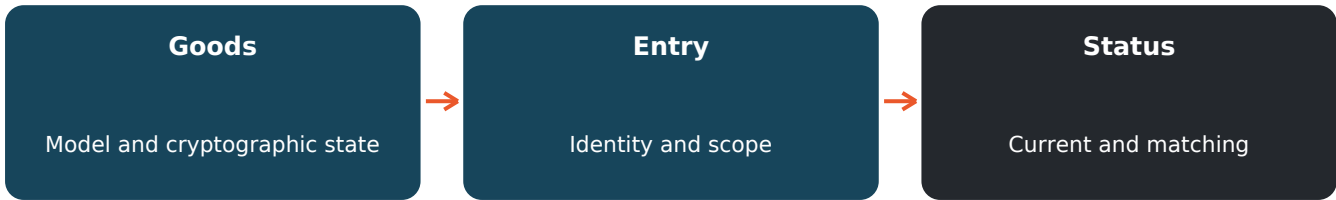
Record updates before closing supply files. Manufacturers describe capabilities and identify affected models. Do not silently extend existing statements with new inputs. Identify old and new software traceably. Assess categories and procedural consequences with competent parties. Prior records remain usable only for matching goods. Version changes alone provide no final legal answer.

In practice

Apply the same technical care to updates as to new variants.

Case: an entry for a similar module

Similar names do not establish reliable coverage.



Product-specific assessment · schematic explanation

Assessment area	Project implementation
Entry	Fictional record for model M-A.
Supply	Model M-B with different firmware and an added function.
Gap	Different identity, functions and parameters.
Resolution	Review complete scope and manufacturer inputs.
Outcome	Coverage unresolved pending reasoned decision.

Purchasing finds an apparently suitable online entry. Engineering compares supplied features. Do not alter model descriptions to manufacture a match. Manufacturer and competent parties establish full coverage. If M-B is outside scope, plan its own eligible route. Keep release unresolved. This example deliberately uses no real registry ID or actual manufacturer goods.

In practice

Bind descriptions to actual goods rather than a desired registry match.

FAQs for manufacturers and importers

Answer frequent questions precisely.

Does every Wi-Fi product need fresh notification?

Not universally. Review scope, capabilities, category, procedure and suitable existing coverage.

Can a foreign manufacturer prepare notification?

Rules provide for manufacturers or authorised persons with special formalities for third-country manufacturers. Confirm actual filing routes.

Does an EAC certificate replace notification?

No. Assess product conformity and non-tariff cryptographic routes separately.

Must specimens always go to a laboratory?

Registration does not establish universal identical specimen or laboratory duties. Necessary clarification depends on goods and procedure.

Is notification effective without registry inclusion?

The reviewed provision connects effect to common registry inclusion. Drafts and filing receipts alone do not establish that effect.

How long is it valid?

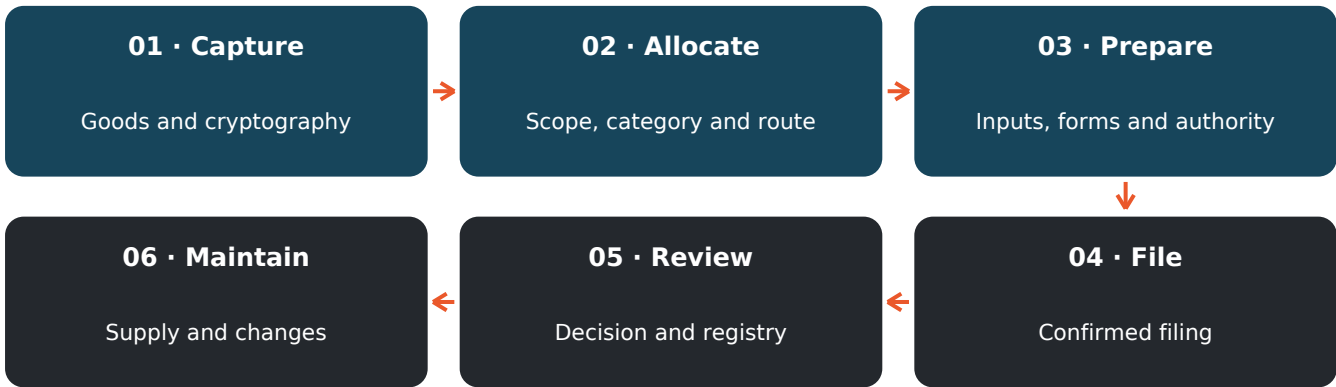
Declared expiry, current status and unchanged functions govern rather than a universal five-year period.

Is 256-bit AES automatically excluded?

No. Review other categories and their complete conditions rather than only parameter category 1.

Costs and reliable project planning

Price technical preparation and formal registration separately.



Assessment area	Project implementation
Inputs	Models, functions, variants and available sources.
Form	Authority, originals, translation and certification.
Procedure	Existing coverage, new notification or alternative route.
Amendment	Clarification and new technical revision.
Schedule	Distinguish overall project and authority phase.

The sector page gives no universal fixed price. Reliable quotations identify models, functions, route, formalities and deliverables. Fresh capability analysis differs from reviewing fully documented existing coverage. Its 20-30 working-day indication is neither statutory timing nor a guaranteed upper limit. Agree start, prerequisites and change triggers. Separate EAC, radio and other services into their own items.

In practice

Quotations need confirmed technical inputs rather than only product names.

Sources: [1]

Worksheet: cryptographic function matrix

Maintain a record for each function and released variant.

Field	Entry / source
Product / model / article	_____
Hardware / firmware / software version	_____
Function / purpose / interface	_____
Protocol / revision	_____
Algorithm / implementation	_____
Maximum key / parameter size	_____
Default / optional capability	_____
Blocking / activation	_____
Radio range / manufacturer input	_____
Category / rationale / reference	_____
Source / date / owner	_____
Approval / unresolved issues	_____

Technical allocation

Do not enter secret keys. Record functions, parameters and confirmed sources.

Enquiry form for your notification project

Provide with available technical records.

Input	Your information
Company / contact	_____
Manufacturer / headquarters / factory	_____
Goods / models / articles	_____
Purpose / use / destination	_____
Tariff / operation / supply scope	_____
Wi-Fi / Bluetooth / other interfaces	_____
Cryptographic functions / algorithms	_____
Maximum key parameters	_____
Software / firmware / options	_____
Existing notification / status	_____
Representative / authority / formalities	_____
Languages / dates / unresolved issues	_____

Attach datasheet, instructions, models, function matrix, software inventory and complete existing evidence. Explicitly identify unavailable inputs.

Contact

info@ac-inorms.com · +49 2161 9904970

Checklist: registration and supply release

Review each supplied revision and actual operation.

Check	Status / evidence
Goods description and tariff confirmed	_____
Complete function inventory	_____
Category conditions substantiated	_____
Existing coverage reviewed	_____
Applicant and authority resolved	_____
Form and translation approved	_____
Consistent manufacturer and models	_____
Filing and clarification recorded	_____
Registry status and expiry checked	_____
Firmware / options match statement	_____
Radio / EAC / other releases checked	_____
Customs linkage / archive / changes secured	_____

Project: _____ Date: _____

Reviewer: _____ Release: _____

Release rule

Assign owners, due dates and closure criteria. This sheet does not replace authority decisions.

Worksheet: form and source reconciliation

Review complete inputs before signature.

Form field	Source / approval
1 · Goods / models / version	_____
2 · Purpose / cryptographic purpose	_____
3 · Manufacturer / contacts	_____
4 · Protocols / algorithms / maxima	_____
4 · Software / range / category	_____
5 · Prescribed additional particulars	_____
6 · Expiry / unchanged-function commitment	_____
7 · Applicant / authorised person	_____
8 · Authority / date / ID	_____
9 · Preparation date	_____
Schedules / signature / form	_____
Registry / actual supplied revision	_____

This is an original review template rather than the official notification form. Use prescribed current forms and accepted national routes for filing. Keep sources, translation and approved goods configurations linked.

Sources and legal foundations

Linked foundations for actual goods and procedure review.

[1] AC Inorms: FSB notification

Open source

[2] AC Inorms: regulations archive

Open source

[3] EAEU: Decision 30/2015, official record

Open source

[4] EEC: Annex 9, cryptographic goods, with 69/2024

Open source

[5] EEC: consolidated Decision 30, amendments through April 2026

Open source

[6] EEC: goods list 2.19, cryptographic means

Open source

[7] EEC: official registry access

Open source

[8] EAEU: common notification registry

Open source

As of 14 October 2026. Reviewed official foundations include [4] and [5]. Registry [8], electronic form and FSB page [9] were unavailable directly for content. No actual registration, current FSB filing address or portal operation is confirmed. Check current channels before filing.

Further sources and image credits

Linked foundations for actual goods and procedure review.

[9] FSB: CLSZ notification information

[Open source](#)

[10] EEC: non-tariff legal foundations

[Open source](#)

[11] EEC: forms and instructions

[Open source](#)

[12] EEC: technical regulations and standards lists

[Open source](#)

[13] European Commission: dual-use exports

[Open source](#)

[14] IETF: RFC 8446, TLS 1.3

[Open source](#)

[15] NIST: FIPS 197, AES

[Open source](#)

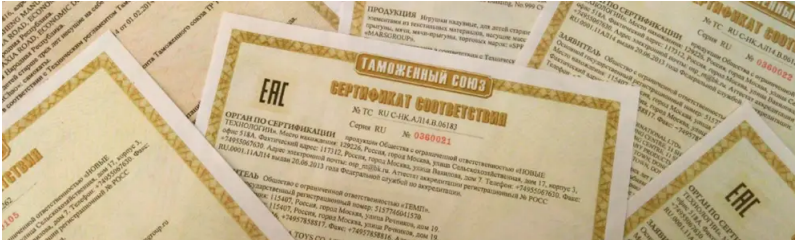
[16] NIST: FIPS 186-5, digital signatures

[Open source](#)

Images: industrial-electronics and explanatory document illustrations from AC Inorms, ac-inorms.com. Diagrams, tables, cases and worksheets are original working aids rather than official forms. Full standards texts are not reproduced. References identify regulatory links; workflows are editorial recommendations.

Your notification project with AC Inorms

Connect technical inputs, formalities and supplies reliably.



Document illustration · not an official notification · AC Inorms

AC Inorms supports goods allocation, cryptographic inventories, record structure, technical translation and coordination of competent procedures. Provide goods, models, firmware, functions, destination and existing notification data for reliable enquiries. These inputs support coverage, formalities, missing manufacturer inputs and further evidence planning. Keep responsibility for manufacturer statements and competent authority decisions clearly allocated.

AC Inorms GmbH

Nobelstraße 3/5 · 41189 Mönchengladbach · Germany

Telephone: **+49 2161 9904970**

Email: **info@ac-inorms.com**

Web: **ac-inorms.com**

For your initial enquiry

Provide the page 45 worksheet with datasheet, models, software inventory and existing evidence.