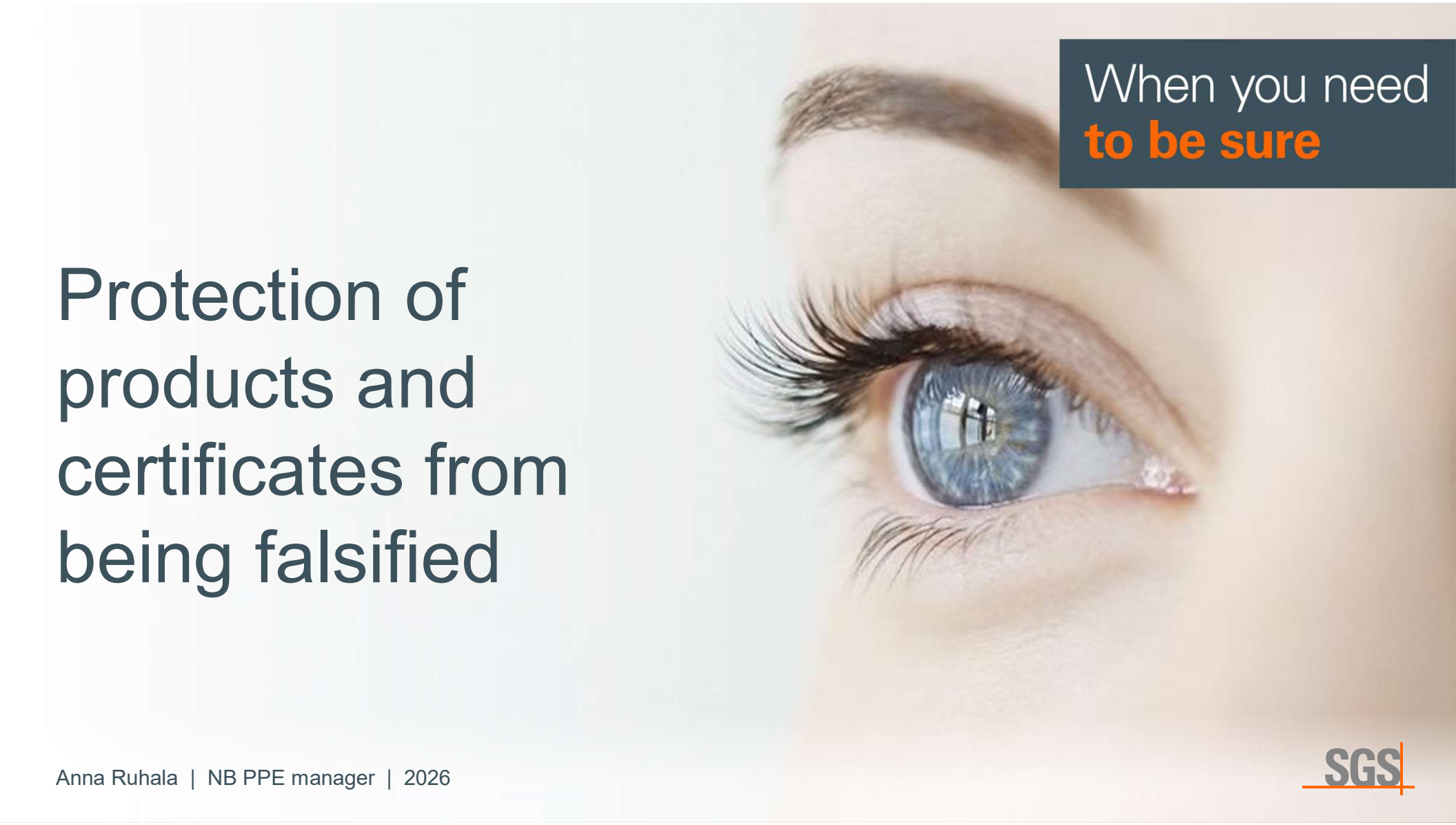
Protection of products and certificates from being falsified



Anna Ruhala | NB PPE manager | 2026

Guest speaker

Anna Ruhala

NB Manager

SGS Fimko Oy

Anna.Ruhala@sgs.com

Anna Ruhala is notified body manager for personal protective equipment (PPE) at SGS Fimko Oy. In her position she is responsible for the global network of PPE experts working under SGS Fimko notified body status. She has over 15 years of experience with PPE – from testing to certification and research to standardization. Anna Ruhala holds an MSc in physics (2007) from the University of Helsinki specializing in material science.

SGS Fimko Oy is part of the global SGS SA group, one of the world's leading testing, inspection and certification companies.

Protection of products and certificates from being falsified

- Falsification of PPE and certificates undermines worker safety, market trust and the credibility of conformity assessment
  - PPE is high-risk: failure directly endangers health and life
  - Distinguish non-compliance vs deliberate falsification
- Problem root: Trust is decentralized; verification is fragmented across borders and actors
- What is being falsified?
  - Product-level
    - Counterfeit PPE
    - Copying CE marking, NB numbers, packaging, IFUs
  - Document-level
    - Forged EU Type-Examination Certificates; misuse of expired/withdrawn certificates; scope mismatches; manipulated test reports
    - *Argument: market actors often check presence of documents, not authenticity*

Why the system is vulnerable

- **Fragmented information** – no unified EU-wide public database for all PPE certificates; verification is slow/uneven
- **Visual trust bias** – paper/PDF artifacts are easy to copy
- **Complex supply chains** – manufacturers, importers, subcontractors, private labels, material/component suppliers, retailers, …
- Market pressure & emergencies – tolerance for risk rises (e.g., pandemics)
- Enforcement remains resource-dependent and reactive

Countermeasures

Where we are now

- PPE Regulation 2016/425 sets obligations
- Market Surveillance Regulation 2019/1020 - enhanced enforcement architecture
- Cooperation: NBs ↔ MSAs ↔ Customs

What more could we do?

- Product-level protection:
  - serialization
  - tamper-evident labels
  - secure marks
  - training of economic operators
- NB actions:
  - post-cert monitoring
  - explicit certificate scopes
- Blockchain
- Digital Product Passport

Blockchain

- What is blockchain?
- Can provide
  - tamper-resistant, time-stamped records
  - distributed verification
- Cannot provide
  - validation of truth of test results
  - physical quality
  - replacement for NBs/MSAs

Blockchain secures claims, not truth – governance remains essential

Blockchain

- High-value use cases
  - **Digital certificates anchored on a ledger**: issuance, scope, suspension, withdrawal, expiry – immutably logged
  - **Lifecycle transparency**: prevents “zombie certificates” (expired/withdrawn resurfacing)
  - **Linking product ↔ certificate** via secure identifiers (QR/Data Matrix/NFC/RFID) for batch/item verification
- Caveat
  - Identifier cloning remains a risk; requires MSA checks and governance to control write-access and validation roles (NBs, MSAs, economic operators).

Digital Product Passport

- A structured digital record linked to a product that shares verified information (identity, composition, traceability, sustainability and relevant compliance/safety data) across the value chain, enabled by the Ecodesign for Sustainable Products Regulation (ESPR) (EU) 2024/1781
- DPPs are accessed via unique identifiers (QR, RFID, NFC) linking to machine-readable data in interoperable systems
- Product-specific data requirements come via delegated/implementing acts
- DPPs are phased by product groups between ~2026–2030, starting with batteries (from Feb 18, 2027) and other priority categories
- PPE is not yet mandated but falls within ESPR's broad scope, so DPP could be extended to PPE in future acts

How DPPs Help Against Falsification

- Declarations of Conformity, EU Type-Examination Certificates, NB details, scope, and status can be embedded/referenced inside the passport as authoritative data – reducing forged or out-of-date documents in circulation
- Faster market checks, automated consistency checks
- ! DPPs don’t guarantee physical performance; identifiers can still be cloned; surveillance and testing remain essential

DPP & Blockchain – How They Fit Together

Pragmatic architecture

- Authoritative DPP registry (EU-level/recognized providers)
- NB-issued digital certificates → hashed/anchored on ledger
- Product identifier links item/batch to DPP entry and certificate references
- Role-based access

DPP = the regulatory data container & access model.

Blockchain = optional trust anchor for high-risk events (issuance/withdrawal logs, custody events).

DPP does not require blockchain but can benefit from it for tamper-evidence and cross-party trust.

Summary

- Falsification of PPE products and documentation is a systemic safety risk; failures can directly endanger health and life.
- Both products and documents are targeted.
- Core weakness: trust is fragmented and authenticity checks are inconsistent across borders and actors.
- No unified EU-wide public database for PPE certificates; verification remains uneven.
- Paper/PDF-based trust is easy to exploit.
- Complex global supply chains and crisis situations increase tolerance for risk.
- Existing regulation (PPE Reg. 2016/425, MSR 2019/1020) provides a baseline, but enforcement is reactive.
- Notified Bodies, MSAs, and Customs cooperation is essential.
- Blockchain can secure claims and events but does not validate product performance or replace oversight.
- DPPs can reduce document falsification by embedding authoritative compliance data, but do not remove the need for surveillance and testing.

No single tool prevents falsification. Layered governance, trusted certification, digital transparency, and active market surveillance must work together.

Questions?

Wind Turbine Inspection, Belgium

Thank you!

Do you have any questions?

Anna.Ruhala@sgs.com
www.sgs.fi