EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 6 · 11 September 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Jessy Lang

You Just... Swapped It?

Seven rules for building the door before you need it

A client swapped its entire encryption scheme in about a week, with zero drama, after Tess flagged a weak algorithm. Nothing about the algorithm was special. The client had built a door: a shared layer, an inventory and a rehearsed rotation path. Strength is a property of today's choice. Agility is a property of how easy tomorrow's choice is.

ASSUMED PERMANENCE
Today's algorithm taken for a fact, not a choice.

1. What do we use, and where?

2. Does it protect a key or the data?

3. Can we swap it without a rewrite?

RULES FOR CRYPTO-AGILITY

1	**A hardcoded algorithm** Names in wire formats, key lengths in schemas, calls in forty files.	Let every service call one shared "encrypt this" function, so the algorithm is a configuration value, not a decision repeated in forty places. The client's layer took a small team about six weeks.
2	**No inventory** Changing an algorithm turns into a scavenger hunt.	Keep a cryptographic bill of materials: which algorithm, which key length, which library, used where, for what. Update it with every change that touches encryption. At another client, with none, a one-week change took four months.
3	**The wrong lock** Swappable means something different for a key and for data.	Use envelope encryption: a data key per record, wrapped by a master key. Swap the wrapping algorithm and re-wrap only the keys, in milliseconds each. Record for every dataset whether an algorithm protects a key or the data itself. Direct encryption took another client the better part of a year.
4	**An untested swap** A procedure invented in the week it is needed.	Exercise the rotation path before you need it. The client had rehearsed it eighteen months earlier for another change. It cost a weekend once, then an afternoon each time. Test in staging, flip, watch the dashboards.
5	**Harvest now, decrypt later** Traffic recorded today is read once a capable quantum computer exists.	Do not wait until the threat is closer, if the data stays valuable for years: health records, trade secrets, government communications. A swap protects envelopes created from today on, never a copy already taken.
6	**The sticker** "Post-quantum" on a product that updated one library.	Do not buy the label, build the capability: the door, the inventory, the tested rotation path. Ask whether the fix only makes sense if one specific threat is real. This one pays off whether the timeline is five years or twenty.
7	**No budget for a door** Six weeks of engineering with no feature to demo.	Pitch flexibility, not defence. Here a customer's contractual wish for a specific algorithm got it approved: security bought the ticket, a sales requirement paid for it. Keep the knowledge written down, not in two engineers' heads.

THREE TAKEAWAYS

Ask what you can still change
Under the Cyber Resilience Act, regulators are starting to ask not what you shipped but what you can still change.

Retire permanent findings
A weak algorithm re-listed year after year becomes wallpaper. Agility attaches a fix to the finding.

Know the limits
Agility does not stop implementation bugs: a bad random number generator, a misplaced key, a side channel.

Listen to the episode
You Just... Swapped It? and the rest of the series.
eacg.de
/en/podcast/s06-crypto-agility

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH