A Lock With No Single Key

Trust, the wallet, and agents in the open 6G network. The sixth and final article in the series

The burglar got lucky. He got everything.

The phone of the doctor from the regional town - the one from the third article in this series. Full access: the wallet that pays for his patients' medications, and the digital agent the doctor launched this morning - to check sensor readings, renew prescriptions, order supplies. The burglar is inside. He opens the wallet.

And finds - nothing.

Not emptiness instead of money. The money is there. Nothing - in a different sense: there is no key in the wallet. No password, no secret phrase, no file that could be copied and carried away. There is only a trace: a commission, signed this morning, permitting the agent exactly three actions for exactly one amount - and expiring in forty minutes. The burglar can, in the agent's name, ask the network to perform one of those three actions. The network will check the commission, execute it, write it into the ledger - and in forty minutes the trace will evaporate. He cannot extend it: that requires something he does not have and will not get.

He broke into one place - and it opened no other.

The Question It All Started With

The five previous articles in this series built an argument: a network without an owner is possible (the ant colony proved it a hundred million years ago), the mechanism for it partially exists (tags in the protocol), it is needed by a specific person (the doctor a base station never reached), three lines in the standard are enough for it (the PQT field, an open format, a hardware signature), and the question about it must be asked where decisions are made.

But a network without a centre has a flip side that has so far been mentioned only in passing. If there is no centre, there is no central vault. No server where the passwords live. No operator to confirm: yes, it is him, let him in. A question arises that sounds simple and is hard to solve: where must trust sit so that breaking any one place requires the impossible - and so that breaking one place does not open the rest?

Notice: these are two different requirements. The first is about strength. The second is about architecture. You can build the strongest safe in the world and fail the second requirement by putting everything into that one safe. That is exactly how most of today's systems are built: one password, one secret phrase, one protected chip - one door, behind which an entire life is kept. For decades the industry has been answering the first question by making the door thicker. Thickness does not answer the second question at all.

A Chord Instead of a Key

The answer that emerged from the work on the open 6G architecture sounds unfamiliar: the lock must have no single key. None at all. Not a thick one, not a thin one, not a hidden one, not one split into shares. The lock opens to a chord - several independent confirmations that must sound together, none of which is a key on its own.

The first note is a chip. A separate secure die that already sits in every phone. It confirms: the request comes from this device.

The second note is geometry. A 6G network can measure a device's position to the centimetre - not by the device's own word, but by the physics of radio propagation, consistently, from several independent relays at once. One antenna can be fooled. Fooling the consistent measurements of three separated nodes means fooling the geometry of space itself.

The third note is the neighbours. Devices nearby - other people's devices, with other owners, other power supplies, other firmware - act as witnesses: yes, we can see this node, it is here, it is behaving as usual. Research on collective attestation established the converse property too: if a node is physically captured and taken out of the network, the neighbours notice its absence. A trace that is no longer reinforced evaporates - and the evaporation itself becomes the alarm. The ant colony from the first article has returned - this time as a burglar alarm.

The fourth note is the person. Their live presence, confirmed the way the Presence Protocol described: not by a password that can be stolen, but by the physiological reality of the moment, which cannot be reproduced once the moment has passed.

No note opens the lock alone. And - this is the point - no two notes share a foundation: they live on different carriers, with different owners, in different physics. The chip can be pried open - the geometry will not flinch. The radio-signal classifier can be confused - the neighbours will not confirm. The phone can be stolen - the person's presence cannot be stolen along with it. The cost of breaking such a system equals not the strength of the thickest door, but the necessity of playing the whole chord at once, on instruments held in different hands.

An Agent That Cannot Be Trusted With Keys - and Does Not Need Them

Now the most interesting part. An agent lives in the wallet - a program that acts on a person's behalf when the person is not around. How do you give it authority without giving it keys?

The old world answers: issue the agent an access token. That is - create a key, put it inside the program, and hope. That is exactly how most software agents are built today, and exactly why breaking them costs so much.

The new answer is different: the agent receives no keys, because no keys exist. The chord of roots - chip, geometry, neighbours, presence - sounds once and signs a mandate: a narrow commission with explicit bounds. What is allowed, how much, until when. The mandate is not

a secret. Stealing it gives the thief only the remainder of the mandate itself: forty minutes and three permitted actions, under an indelible ledger. The mandate cannot be widened - the mathematics of its construction allows authority only to narrow. The mandate cannot be extended - renewal requires a new chord. And the mandate evaporates on its own - like a pheromone trail no longer reinforced, like the path-quality tag in the protocol whose time-to-live has run out. One and the same architectural move runs through the entire series: memory and authority are kept in time, not in a vault.

And there is a final line of defence, the deepest one. In this architecture the agent is deprived of the ability to act at all. It can only propose: it publishes an intent, and independent nodes of the environment execute it - each one checking the intent against the mandate before executing. This is not futurology: the world of smart accounts already works this way - the agent proposes, the policy and the wallet execute within hard limits, and by mid-2026 such accounts number in the tens of millions. A hacked agent in this model is a burglar who can only ask.

Security as Emptiness

Notice what has happened to the very notion of protection. We are used to thinking of security as armour: thicker walls, longer ciphers, stronger safes. That whole logic answers the question “how to make a break-in impossible” - and loses on the day the break-in happens anyway, because behind the armour everything is kept in one place.

The architecture described in this series answers a different question: how to make a break-in useless - and visible. A root falls - certification has already rehearsed this, deliberately breaking each root in turn and checking that the neighbouring ones did not flinch. A device is captured - the neighbours noticed the absence of its trace. An agent is hacked - it can only ask. The structure of the system is known to everyone - and that is precisely why it says nothing about anyone: when all devices of a class are built identically, knowing the design stops being loot. Anonymity loves company.

The burglar from the beginning of this article met no impenetrable wall. He met no wall at all. He walked in - and discovered that nothing worth coming for was kept inside. That is the lock with no single key: not a fortress, but an emptiness with nothing to take.

Closing the Series

Six articles - one argument.

A network can have no owner - because the environment owns the memory. The mechanism for this is the tag every packet leaves behind. It is needed by a specific person - the doctor, the farmer, the teacher, whom the centre's commercial arithmetic never reaches. Three lines in the standard are enough for it. The question about them must be asked where decisions are made. And finally - in such a network there is someone to trust and a way to trust: trust sits in independent roots that share no foundation, and everything else - agents, mandates, authority - is only the evaporating traces of that trust.

The doctor in the regional town does not know the word “quorum” and will never read a single contribution to a standard. He knows something else: the signal from his patient's sensor arrived in time. And when his phone was stolen - the next day, with a new device, everything restored itself, and nothing was lost. Because there was nothing in the stolen phone that could be carried away.

The 6G standards are being finished now. The window every article in this series spoke of is still open - but it is closing. When it closes, the architecture will reproduce itself for twenty years ahead - through equipment, through regulation, through the habits of billions of people.

The future network can have a centre, a vault, and a single key. Or it can have a chord, a trace, and an emptiness with nothing to steal.

A lock with no single key cannot be opened by a stranger's hand. But it can still be built.

This is the sixth and final article in a series on the design of next-generation networks. The technical foundations are set out in the contributions to IEEE IC25-009-01: the Presence Protocol, the Accountability Chain Protocol (ACP), the Independence-of-Foundations Principle (P-INDEP), and the resolution of its open questions together with the P-DELEG delegation principle.