Towards a privacy-preserving PKI for Satellite Communications

Arlette Houndji[1,2,4][0009−0006−8803−9007], Alfonso Iacovazzi[1][0000−0001−6116−164X], Jaap-Henk Hoepman[2,3][0000−0003−4234−1578], Simone Fischer-Hübner[2][0000−0002−6938−4466], and Shahid Raza[1,4][0000−0001−8192−0893]

[1] Research Institutes of Sweden, 16440 Stockholm , Sweden
[2] Karlstad University , 65188 Karlstad, Sweden
[3] Radboud University, 6525 XZ Nijmegen, Netherlands
[4] University of Glasgow, G12 8RZ Glasgow, UK
{arlette.houndji,alfonso.iacovazzi}@ri.se
simone.fischer-huebner@kau.se
jhh@cs.ru.nl
shahid.raza@glasgow.ac.uk

Abstract. The rapid deployment of Low Earth Orbit (LEO) satellite constellations is revolutionizing satellite communications (SATCOM). Mainly, securing direct to device communications in SATCOM introduces some privacy challenges that conventional Public Key Infrastructure (PKI) solutions cannot fully address. This is due to the unique characteristics of space networks, including highly dynamic topologies, mobility, and resource constraints. In this paper we present a PKI scheme which leverages the use of unlinkable credentials, lightweight C509 certificates, and the EDHOC (Ephemeral Diffie-Hellman Over COSE) protocol for privacy-preserving PKI.

Keywords: PKI · SATCOM · LEO · Privacy · Unlinkability · Pseudonyms · Blind Signatures · C.509 · EDHOC

1 Introduction

The emerging "New Space", characterized by the involvement of private companies and entrepreneurs in space exploration and technology, has set a new pace for the development of satellite communications (SATCOM) [12]. The deployment of Low Earth Orbit (LEO) constellations and the native integration of terrestrial and non-terrestrial networks in 6G [23] are transforming global connectivity, and SATCOM now serves platforms and users, well beyond broadcast applications. Public Key Infrastructure (PKI) serves as a cornerstone of security on the terrestrial Internet, where it ensures authentication, confidentiality, and integrity. Using a PKI in satellite networks, however, raises new challenges [14,24]: *(i)* the resource and bandwidth cost of classical certificate formats and enrollment protocols in a constrained environment; *(ii)* the inconvenience of having static trust anchors in

a highly mobile, multi-operator environment where handovers are frequent; and *(iii)* the privacy exposure of long-lived certificates, which enable cross-operator tracking and profiling of end users as they connect across constellations. To illustrate these challenges, we describe a use case around a drone dispatched in a region where terrestrial connectivity is absent or hostile. This drone must periodically deliver telemetry data to a backend command center through a LEO satellite. Every data transfer begins with a mutual authentication between the drone and a satellite, which can be repeated multiple times over a mission across satellites that may belong to different operators in different jurisdictions. We develop the scenario in detail in Section 3.

The key research question we address in this paper is how to design a PKI for SATCOM that provides mutual authentication and key establishment while preventing any observer from tracking a mobile terminal, in this case a drone, across its successive connections. Our solution adapts the pseudonym-based architecture of vehicular PKI [25,3] to PKI in SATCOM systems. The main contribution is a privacy-preserving PKI scheme using blindly issued pseudonym batches, compact certificates, and a lightweight authenticated key exchange.

The remainder of the paper is organised as follows: Section 2 provides background and related work. Section 3 presents the system model, the use case, the adversary model, and the design goals. Section 4 describes the proposed scheme. Section 5 revisits the design goals and shows how each is met. Section 6 concludes the paper.

2 Background

PKI. A PKI is a framework that uses public key cryptographic techniques to secure digital communications and authenticate the identities of users and devices [11]. The framework involves a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates [10]. The main function of a PKI is to verify public keys of entities and prove their trustworthiness. RFCs 5280, 2560, 3647, [2,9,8] are a few standard documents describing the technical specifications of the PKI framework, and the PKI certificate management structure.

Certificates. Classical X.509 certificates [2] were designed for the terrestrial Web PKI and carry a non-negligible overhead in both size and parsing cost. Recent work on CBOR-encoded *C.509* certificates [17] preserves the X.509 trust model while substantially reducing size, making it more suitable for satellite terminals and inter-satellite links.

Location privacy. According to Liu et al. [15], location privacy is defined as the protection of an individual's location information from unauthorized access and misuse, ensuring that users can control who knows their location and when [15]. In this paper, we primarily focus on the unlinkability, pseudonymity, and confidentiality aspects of location privacy. We have identified two (02) primary

threats to location privacy: (i) device identity leakage, where a device's unique identifiers are exposed; and (ii) metadata analysis, where certificate issuance and use,timing, and frequency can be analyzed to infer the location of the device.

Linkability. Two items are linkable for an attacker if that attacker can determine, from what it observes, whether they relate to the same entity [20]. Unlinkability is therefore not an absolute property of a credential but a property relative to a particular observer and its accumulated observations. In mobile environments, the properties are position observations, and linking a sequence of them yields a trajectory that identifies launch points, destinations, and behavioural patterns [22].

Anonymity. Anonymity is the property of not being identifiable within a set of subjects, called the anonymity set [20]. It is not binary but graduated, and the standard measures quantify it by the size of that set or by the entropy of the attacker's probability distribution over its members [21,7]. The idea traces to Chaum's mix networks, which hide the correspondence between inputs and outputs by batching and reordering traffic [5]. Pseudonymity sits between full identification and anonymity, since a pseudonym carries no identity but does accumulate a history of its own uses [20]. Anonymous credentials push closer to the anonymous end by letting an entity prove that it holds a valid credential without revealing which one it holds [4,16]. Anonymous credential enable selective disclosure allowing users to choose which specific attributes to share and hide the rest during verification. Moreover, unlinkability of different credential shown can be enabled.

Blind signatures. Blind signatures allow a signer to sign a message without seeing it, a primitive Chaum introduced for untraceable electronic payments [6]. The property that matters for privacy is that the signer cannot afterwards associate a signature it encounters in use with the session in which it produced it.

3 System and Threat Model

3.1 System Overview

In this paper, we consider drones as the security sensitive end users of the system. Each drone is a mobile platform that periodically transmits mission data to an authorized end device or service using the satellite network. The position of drones is sensitive information that can be used to perform malicious actions. An adversary that can correlate successive transmissions to and from a single drone learns a movement trace, which may reveal mission objectives or allow to track the drone as it moves.

Use case: To describe the threat model, we walk through a scenario that exercises every privacy property the scheme provides. A reconnaissance drone is sent by its home nation on a military intelligence gathering mission over contested territory. The drone must periodically transmit telemetry and sensor data to a command center operated by its home nation. Terrestrial infrastructure in the operating area is unavailable or presumed hostile, a situation that has become more prevalent in recent conflicts, where commercial LEO constellations have served as primary connectivity for military and dual-use platforms [18]. The satellite is therefore the drone's only channel to its backend. At each reporting interval the drone performs mutual authentication with a satellite in the constellation, and transmits data destined for the command center. A LEO satellite remains in view for a few minutes at most, so a reporting session may require a handover from one satellite to its successor, and a mission lasting hours will involve many independent authentication events spread across satellites that may belong to different operators in different jurisdictions. The PKI comes into play because both endpoints of every one of those authentication events need cryptographic assurance about the other. The satellite must verify that the transmitting party is a legitimate subscriber and not a spoofed emitter attempting to inject traffic or exhaust resources, given how exposed satellite links are to attackers [19]. The drone must verify that the party it is about to hand mission data to is a satellite of an authorized constellation and not an adversarial actor imitating one. Certificates, a chain of trust, and a revocation mechanism are a standard solution for this in terrestrial networks, and Section 4 adapts it to the constraints of the setting.

Each drone holds a long-term cryptographic identity issued at provisioning and uses short-lived pseudonym certificates for all communications during the mission. Satellites form a LEO constellation, possibly federated across multiple operators, and act as relays between drones and the ground segment. From the drone's point of view, the satellite is the first peer it authenticates to during a session. Satellites are connected via inter-satellite links (ISLs). We make no assumption that satellites are tamper-proof or that operators are mutually trusting. The ground infrastructure hosts the certification authorities, and the space infrastructure can issue additional pseudonyms to drones out the terrestrial coverage area. The ground infrastructure consists of a Long-Term Certificate Authority (LTCA), which issues long-term identity certificates to drones at enrollment, and a Pseudonym Certificate Authority (PCA), which issues batches of short-lived pseudonymous certificates that drones use during missions. Optionally, a Resolution Authority (RA) may be added to bind a pseudonym back to its long term identity in case of abuse. Figure 1 shows a depiction of the scenario.

3.2 Trust assumptions

The LTCA is trusted to correctly bind enrollment identities to the drone's public keys. It is the only entity that knows the long-term identity of each drone. The PCA is trusted to correctly issue short-lived pseudonym certificates from valid requests authorized by the LTCA, but it is not trusted with the binding between a

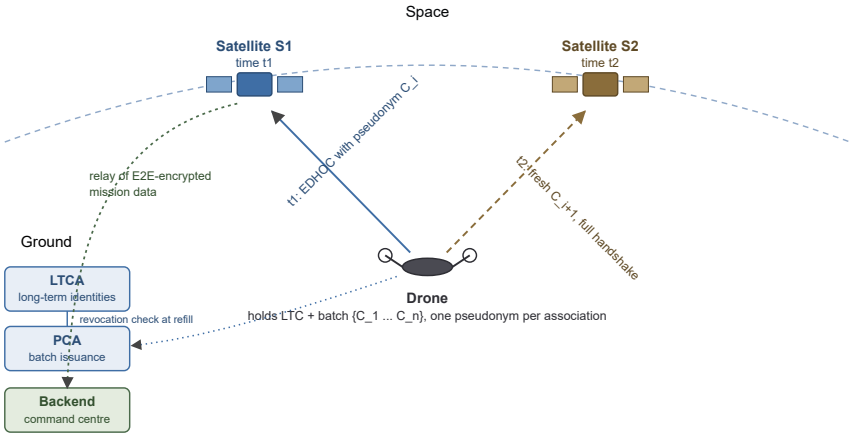

Fig. 1. Use Case

drone's long-term identity and the pseudonyms it issues. We enforce this property cryptographically through blinded issuance, as described in Section 4.3. Drones are trusted to keep their long-term and pseudonym private keys secure. Satellites and their operators are modeled as *honest-but-curious*. They correctly execute the protocol, but can log all authentication operations.

3.3 Adversary model

We consider an adversary $\mathcal{A}$ with the following capabilities. A curious adversary may control a subset of satellites and their associated ground infrastructure, logging all authentication material visible to those satellites and attempting to correlate observations across them. We assume $\mathcal{A}$ does not control the LTCA or the PCA. $\mathcal{A}$ may compromise a certain number of drones and obtain their long-term and pseudonym certificates. This must not affect the privacy of other drones. State adversaries capable of compromising the LTCA or PCA, side-channel attacks on drone hardware, and traffic-analysis attacks based on physical layer fingerprinting of drone radios are not considered.

3.4 Security and privacy goals

– **(G1) Mutual authentication:** a drone and a satellite must mutually authenticate before any mission data is exchanged.

- **(G2) Confidentiality and integrity:** mission data must be confidential and protected end-to-end between the drone and the authorized backend consumer. Intermediate satellites must not be able to read or modify it.
- **(G3) Pseudonym unlinkability:** no curious operators can determine whether two authentication sessions correspond to the same drone.
- **(G4) Location privacy:** as a consequence of G3, no such operator may reconstruct the movement trace of any specific drone, even when the drone hands over across satellites of different operators within a single mission.
- **(G5) Accountability:** optionally, the LTCA in cooperation with the PCA and the RA, may resolve a pseudonym back to its long-term identity when investigating abuse.

3.5 Linkability requirements vs privacy credentials

The privacy preserving authentication system we describe is designed against two main requirements. On one hand is linkability, where every authentication event carries a persistent identifier and the verifier can connect sessions of the same device. On the other hand there is full anonymity, where no verifiers and issuers can connect any two sessions, and where no party can answer the question of who performed a given authentication.

The difficulty is that several functional requirements of a deployment have linkability requirements, and revocation is an example. To revoke a misbehaving device is to ensure that all of its future credentials are rejected, and doing so requires that some party be able to connect those credentials to the device. Sybil resistance is a second example. Guaranteeing that one enrolled device cannot authenticate as fifty different devices simultaneously requires that some party be able to bound the number of live credentials per enrolled identity, which is a form of linkage at the issuer. Conditional accountability, our goal **G5**, is a third. Auditing after documented abuse requires a path from a pseudonym back to an identity, and that path is a linkage that must exist somewhere, held by someone, under some governance. For this, we propose having a separate secret sharing scheme for accountability, so that linkage needs to be decided and done by more than one party, following the four eyes principle. A more detailed discussion will follow in the final paper.

The design question is therefore not only whether linkage exists but where it is located, who can compute it, and under what conditions. We find it useful to distinguish four locations. Linkage may exist at the *verifier*, meaning satellites can connect sessions on their own, which is the scenario we are working to prevent. It may exist at the *issuer*, meaning the PCA can connect the credentials it issued to the identity that requested them, which blinded issuance eliminates. It may exist at a third-party authority, where a party such as the RA holds a secret that converts pseudonyms to identities under a controlled procedure, which is the optional accountability mode of Section 4.3. Or it may exist *nowhere*, which maximises privacy but removes accountability. Our scheme places Sybil resistance at the issuer, since the PCA bounds batch sizes per valid long-term certificate without learning the pseudonym contents, places revocation at the issuer as well,

since refills are denied to revoked long-term identities, and makes third-party authority linkage a deployment choice rather than a fixed property.

4 Proposed scheme

We now describe the proposed privacy preserving PKI scheme for SATCOM. The scheme adapts a Vehicular PKI (VPKI) model originally developed for vehicular networks [3] to the SATCOM setting, retaining the long-term certificate and pseudonym certificate separation. Figure 2 shows a sequence diagram of the scheme.

4.1 Architecture

The architecture comprises the three certification authorities introduced in Section 3, the LTCA, the PCA, and optionally the RA.

We deliberately omit the Linkage Authorities (LAs) that appear in SCMS [25,3]. LTCA revocation cuts off a misbehaving drone within one batch cycle, because the drone can no longer refill. Also, pseudonym unlinkability in our scheme is provided by blinded issuance. Adding LAs would introduce extra costs. We note that Simplicio et al. [13] reach a similar conclusion for revocation, showing that LA roles can be securely decentralized.

All certificates issued, both long-term and short-lived pseudonym, use the C.509 format [17] rather than X.509. C.509 preserves X.509 trust semantics and validation logic while reducing on-the-wire size, which is particularly significant when issuing pseudonyms in batches over a satellite link and when verifying them on constrained satellite hardware.

4.2 Enrollment

Enrollment is the procedure by which a drone obtains its long-term identity. It is performed before deployment over a trusted link, and is therefore not subject to the bandwidth and connectivity constraints of the in-mission phase. The drone generates a key pair $(sk_{\mathrm{LT}}, pk_{\mathrm{LT}})$ locally and submits a Certificate Signing Request (CSR) to the LTCA. The LTCA verifies the drone's attestation supplied by the manufacturer, binds pk_{LT} to a unique identifier, and issues a long-term C.509 certificate C_{LT}. The drone stores $(sk_{\mathrm{LT}}, C_{\mathrm{LT}})$ in its local storage. The LTCA retains C_{LT} in its enrollment database.

4.3 Pseudonym batch issuance

Pseudonym issuance is the mechanism through which the drone obtains a batch of n short-lived pseudonymous certificates from the PCA. The protocol is designed so that the PCA does not learn the binding between the drone's long-term identity and the pseudonyms it issues, which is the property that enables **G3**. The drone generates n fresh pseudonym key pairs $\{(sk_i, pk_i)\}_{i=1}^{n}$. For each key

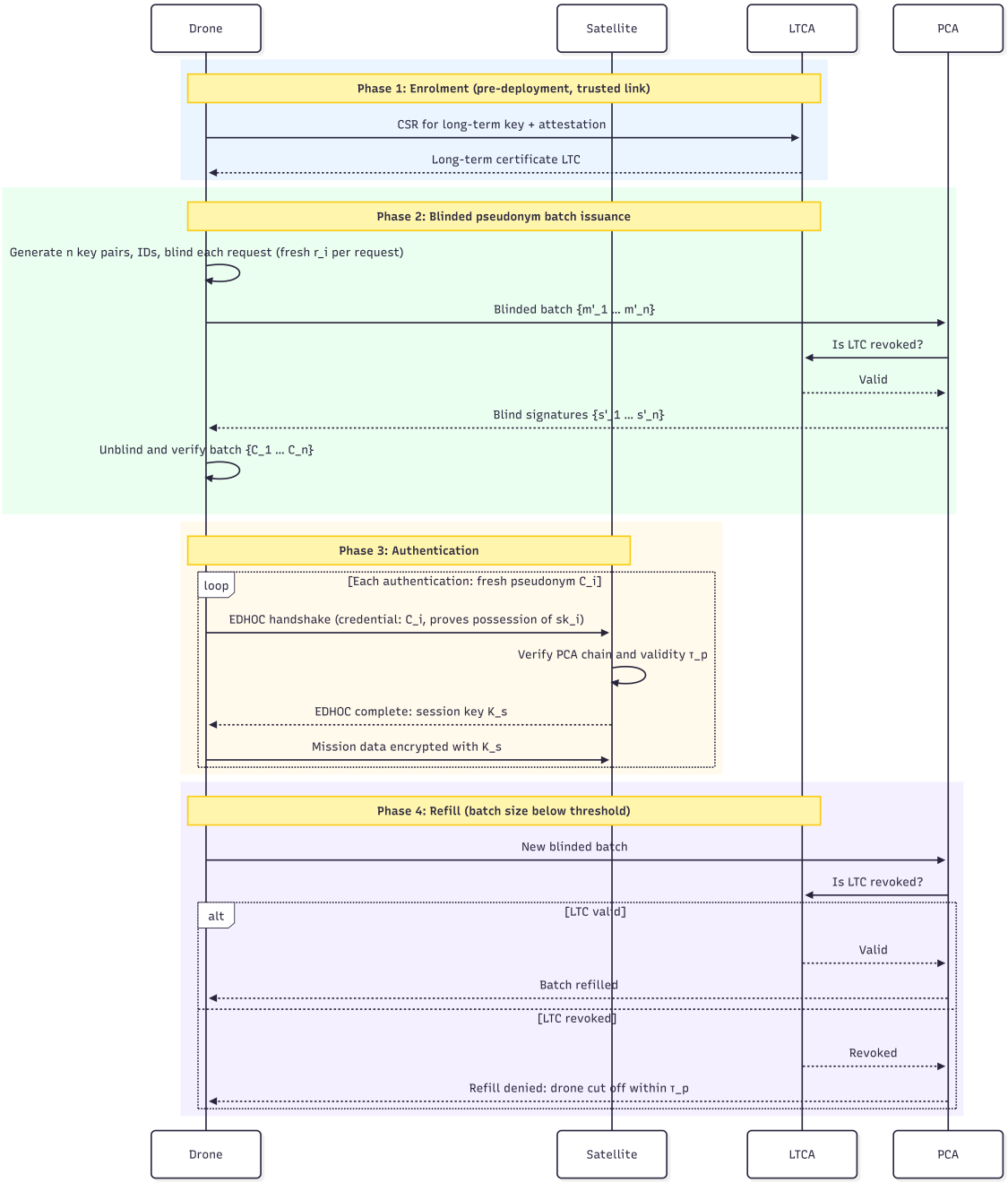

Fig. 2. Sequence Diagram

Algorithm 1 Pseudonym batch issuance (drone side)

Require: Long-term credential $(sk_{\mathrm{LT}}, C_{\mathrm{LT}})$; PCA public key pk_{PCA}; batch size n; validity period τ_p
Ensure: Batch $\{(sk_i, C_i)\}_{i=1}^{n}$ of pseudonym key pairs and certificates

$B \leftarrow \emptyset$; $R \leftarrow \emptyset$ ▷ blinded batch; blinding factors kept locally
for $i = 1$ to n **do**
  $(sk_i, pk_i) \leftarrow \mathsf{KeyGen}()$
  $ID_i \leftarrow \mathsf{RandID}()$
  $req_i \leftarrow (ID_i, pk_i, \tau_p)$
  $r_i \leftarrow \mathsf{RandBlind}()$
  $req'_i \leftarrow \mathsf{Blind}(req_i, r_i, pk_{\mathrm{PCA}})$
  $B \leftarrow B \cup \{req'_i\}$; $R \leftarrow R \cup \{(i, r_i)\}$
end for
Authenticate to PCA
Send B to PCA
▷ PCA verifies C_{LT} against LTCA revocation list; entitlement to size n;
▷ signs each $req'_i \in B$ under sk_{PCA}
Receive $\{\sigma'_i\}_{i=1}^{n}$ from PCA
for $i = 1$ to n **do**
  $\sigma_i \leftarrow \mathsf{Unblind}(\sigma'_i, r_i, pk_{\mathrm{PCA}})$
  if $\mathsf{Verify}(pk_{\mathrm{PCA}}, req_i, \sigma_i) = \perp$ **then**
    abort ▷ malformed signature; batch is discarded
  end if
  $C_i \leftarrow \mathsf{EncodeC509}(req_i, \sigma_i)$
end for
return $\{(sk_i, C_i)\}_{i=1}^{n}$

pair it constructs a pseudonymous CSR and blinds it individually with its own fresh blinding factor. The batch is thus n instances of a blind signature protocol rather than a single blinding of the whole batch, and the independence of the n blinding factors is what makes the resulting certificates mutually unlinkable from the PCA's point of view. We instantiate the blind signature with the RSA construction of Chaum [6], proven secure under the one-more-RSA assumption [1]. The drone then sends the blinded batch request to the PCA. The PCA verifies that the requesting drone holds a valid long-term certificate and that it is entitled to a batch of size n, then issues n blind signatures on the batch. The PCA learns that a drone has requested n pseudonyms, but not which long-term identity the resulting pseudonyms correspond to. The drone unblinds the responses to obtain n pseudonymous C.509 certificates $\{C_i\}_{i=1}^{n}$. Both the pseudonym key pair and the pseudonym are generated by the drone, and this choice is forced by the privacy requirement.

4.4 Authentication

During a mission, the drone authenticates to each satellite using a fresh pseudonym from its batch. Authentication is performed using EDHOC (Ephemeral Diffie-

Hellman Over COSE), which provides a compact authenticated key exchange suitable for the bandwidth budgets of constrained satellite links and supports raw public keys as well as C.509 credentials natively. The drone selects an unused pseudonym certificate C_i from its batch and runs EDHOC with the overhead satellite, presenting C_i as its credential. The satellite verifies C_i by validating its chain to the PCA's public key. On successful completion, drone and satellite share a symmetric session key K_s that is used to protect the subsequent data exchange between them. Mission data carried over the resulting channel is additionally end-to-end encrypted under the backend consumer's public key before transmission, so that the satellite acts only as a confidential relay **(G2)**. The pseudonym C_i is retired immediately after use. It is never presented twice, even to the same satellite, and even within a single mission. When the drone hands over from one satellite to the next, it presents a different pseudonym C_{i+1}, which is unlinkable to C_i from the perspective of any party other than the drone itself.

4.5 Pseudonym Refill

The drone uses pseudonyms at the rate of at least one per satellite association. When the remaining batch falls below a threshold n_{low}, the drone initiates a refill. Refill follows the same blinded protocol as initial issuance. We model refill as a three-phase interaction: request submission, PCA processing, and batch retrieval. The choice of batch size n and refill threshold n_{low} is a deployment parameter that trades off storage on the drone and pseudonym-staleness against refill frequency. These will be analysed further in the final paper.

4.6 Revocation

Revocation in the scheme operates at two layers. For the long-term identifiers, the LTCA maintains a revocation list of compromised or decommissioned drones. This list is consulted by the PCA at the time of every pseudonym issuance and refill request, and prevents a revoked drone from obtaining new pseudonyms. For pseudonym certificates, their short validity time is used. When a drone has its long-term identity revoked, it retains only the unused pseudonyms in its current batch. Each of these expires within at most the pseudonym lifetime τ_p, and once expired it is rejected by any satellite upon validity check. The pseudonym lifetime τ_p is itself a privacy parameter. Shorter τ_p improves unlinkability, since fewer authentication events occur under a given pseudonym, but increases refill frequency and therefore enrollment overhead. We also treat τ_p as a deployment parameter to be analysed quantitatively in the final paper.

5 Security Analysis

We now revisit the goals of Section 3.4 and show how the scheme meets each of them.

G1, mutual authentication. Every association begins with an EDHOC handshake in which both sides present certificates. The satellite presents its credential, and the drone presents a pseudonym certificate C_i signed by the PCA.

G2, confidentiality and integrity. The EDHOC handshake yields a fresh session key K_s per association. Mission data is additionally encrypted using the backend consumer's public key before it is sent, so the satellite relays the data and cannot read or modify. Compromise of a satellite therefore exposes no mission conten.

G3, pseudonym unlinkability. Unlinkability is enforced at both ends of a pseudonym's life. At issuance, each CSR is blinded with an independent random factor, so the PCA signs without seeing the pseudonym key or identifier, and it cannot associate any certificate later observed in use with any issuance session it served.

G4, location privacy. Since each association uses a fresh pseudonym that no coalition can link to any other (G3), the observations available to such a coalition form an unordered set of anonymous events. What remains observable is aggregate activity, namely how many connections occurred in an area over a time window, which bounds fleet activity but attributes nothing to any individual drone.

G5, accountability. A proposed extension for conditional accountability will be provided in the final paper.

6 Conclusion

Satellites are increasingly used in scenarios where there is limited access to ground network infrastructures, and security is a focal point. We have presented a privacy preserving PKI scheme for SATCOM in which drones authenticate to satellites using short-lived pseudonymous certificates issued in blinded batches, so that the drones are not tracked by a malicious observer. The use of compact C.509 certificates and the lightweight EDHOC key exchange keeps the resource and bandwidth use to a minima. In future work, we will perform a formal security and privacy analysis and a performance evaluation quantifying issuance, authentication, and refill costs under realistic conditions. We will also examine the use of anonymous credentials as a means to further improve unlinkability.

References

1. Bellare, M., Namprempre, C., Pointcheval, D., Semanko, M.: The one-more-RSA-inversion problems and the security of chaum's blind signature scheme. Journal of Cryptology **16**(3), 185–215 (2003). https://doi.org/10.1007/s00145-002-0120-1
2. Boeyen, S., Santesson, S., Polk, T., Housley, R., Farrell, S., Cooper, D.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (May 2008). https://doi.org/10.17487/RFC5280, https://www.rfc-editor.org/info/rfc5280

3. Brecht, B., Therriault, D., Weimerskirch, A., Whyte, W., Kumar, V., Hehn, T., Goudy, R.: A security credential management system for V2X communications. IEEE Transactions on Intelligent Transportation Systems **19**(12), 3850–3871 (2018). https://doi.org/10.1109/TITS.2018.2797529
4. Camenisch, J., Lysyanskaya, A.: Signature schemes and anonymous credentials from bilinear maps. In: Annual international cryptology conference. pp. 56–72. Springer (2004)
5. Chaum, D.: Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM **24**(2), 84–90 (1981). https://doi.org/10.1145/358549.358563
6. Chaum, D.: Blind signatures for untraceable payments. In: Advances in Cryptology. pp. 199–203. Springer (1983)
7. Díaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In: Privacy Enhancing Technologies (PET 2002). LNCS, vol. 2482, pp. 54–68. Springer (2003). https://doi.org/10.1007/3-540-36467-6_5
8. Ford, D.W.S., Chokhani, D.S., Wu, S.S., Sabett, R.V., Merrill, C.C.R.: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. RFC 3647 (Nov 2003)
9. Galperin, S., Adams, D.C., Myers, M., Ankney, R., Malpani, A.N.: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 2560 (Jun 1999). https://doi.org/10.17487/RFC2560, https://www.rfc-editor.org/info/rfc2560
10. Hunt, R.: Pki and digital certification infrastructure. In: Proceedings. Ninth IEEE International Conference on Networks, ICON 2001. pp. 234–239 (2001). https://doi.org/10.1109/ICON.2001.962346
11. IBM: What is public key infrastructure? (2023), https://www.ibm.com/think/topics/public-key-infrastructure, accessed on November 07, 2024
12. J. Homans, S.T.: The new space race (2024), https://www.taylorwessing.com/en/interface/2024/the-space-race/the-new-space-race-outlook-and-opportunities-in-2024, accessed on November 06, 2024
13. Jr., M.A.S., Cominetti, E.L., Patil, H.K., Ricardini, J.E., Silva, M.V.M.: A privacy-preserving method for temporarily linking/revoking pseudonym certificates in VANETs. IACR Cryptology ePrint Archive **2018/788** (2018), https://eprint.iacr.org/2018/788
14. Koisser, D., Mitev, R., Yadav, N., Vollmer, F., Sadeghi, A.R.: Orbital trust and privacy: SoK on PKI and location privacy challenges in space networks. In: 33rd USENIX Security Symposium (USENIX Security 24). pp. 6093–6111. USENIX Association, Philadelphia, PA (Aug 2024), https://www.usenix.org/conference/usenixsecurity24/presentation/koisser
15. Liu, B., Zhou, W., Zhu, T., Gao, L., Xiang, Y.: Location privacy and its applications: A systematic study. IEEE Access **6**, 17606–17624 (2018). https://doi.org/10.1109/ACCESS.2018.2822260
16. Martucci, L.A., Kohlweiss, M., Andersson, C., Panchenko, A.: Self-certified sybil-free pseudonyms. In: Proceedings of the First ACM Conference on Wireless Network Security. p. 154–159. WiSec '08, Association for Computing Machinery, New York, NY, USA (2008). https://doi.org/10.1145/1352533.1352558, https://doi.org/10.1145/1352533.1352558
17. Mattsson, J., Selander, G., Raza, S., Höglund, J., Furuhed, M.: Cbor encoded x.509 certificates (2024), https://www.ietf.org/archive/id/draft-ietf-cose-cbor-encoded-cert-07.html, iETF

18. Pavur, J., Martinovic, I.: SoK: Building a launchpad for impactful satellite cybersecurity research. In: Proceedings of the 2022 Workshop on Security of Space and Satellite Systems (2022), arXiv:2010.10872
19. Pavur, J., Moser, D., Strohmeier, M., Lenders, V., Martinovic, I.: A tale of sea and sky: On the security of maritime VSAT communications. In: 2020 IEEE Symposium on Security and Privacy (S&P). pp. 1384–1400 (2020). https://doi.org/10.1109/SP40000.2020.00056
20. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. Tech. rep., TU Dresden and ULD Kiel (2010), version 0.34
21. Serjantov, A., Danezis, G.: Towards an information theoretic metric for anonymity. In: Privacy Enhancing Technologies (PET 2002). LNCS, vol. 2482, pp. 41–53. Springer (2003). https://doi.org/10.1007/3-540-36467-6_4
22. Shokri, R., Theodorakopoulos, G., Boudec, J.Y.L., Hubaux, J.P.: Quantifying location privacy. In: 2011 IEEE Symposium on Security and Privacy (S&P). pp. 247–262 (2011). https://doi.org/10.1109/SP.2011.18
23. Union, I.T.: Framework and overall objectives of the future development of imt for 2030 and beyond (2023), https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2160-0-202311-I!!PDF%-E.pdf, accessed on November 06, 2024
24. Wang, J., Zhang, Y., Zhao, S., He, J., Shen, Y., Jiang, X.: A survey on authentication in satellite internet. In: Journal of Networking and Network Applications, Volume 2, Issue 4. p. 183–194 (2022), https://doi.org/10.33969/J-NaNA.2022.020406
25. Whyte, W., Weimerskirch, A., Kumar, V., Hehn, T.: A security credential management system for V2V communications. In: 2013 IEEE Vehicular Networking Conference (VNC). pp. 1–8. IEEE (2013). https://doi.org/10.1109/VNC.2013.6737583