

RATS Working Group
Internet-Draft
Intended status: Informational
Expires: 7 March 2026

H. Birkholz
Fraunhofer SIT
C. Newton
L. Chen
University of Surrey
T. Giannetsos
Ubitech
D. Thaler
Microsoft
3 September 2025

Direct Anonymous Attestation for the Remote Attestation Procedures
Architecture
draft-ietf-rats-daa-08

Abstract

This document maps the concept of Direct Anonymous Attestation (DAA) to the Remote Attestation Procedures (RATS) Architecture. The protocol entity DAA Issuer is introduced and its mapping with existing RATS roles in DAA protocol steps is specified.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-rats-daa/>.

Discussion of this document takes place on the Remote Attestation Procedures (rats) Working Group mailing list (<mailto:rats@ietf.org>), which is archived at <https://mailarchive.ietf.org/arch/browse/rats/>. Subscribe at <https://www.ietf.org/mailman/listinfo/rats/>.

Source for this draft and an issue tracker can be found at <https://github.com/ietf-rats-wg/draft-ietf-rats-daa>.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 March 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Terminology	3
3. Direct Anonymous Attestation	4
4. DAA changes to the RATS Architecture	6
5. Additions to Remote Attestation principles	7
6. Implementation Status	8
6.1. Implementer	8
6.2. Implementation Name	8
6.3. Implementation URL	8
6.4. Maturity	8
6.5. Coverage and Version Compatibility	9
6.6. License	9
6.7. Implementation Dependencies	9
6.8. Contact	9
7. Privacy Considerations	9
8. Security Considerations	9
9. Implementation Considerations	10
10. References	10
10.1. Normative References	10
10.2. Informative References	11
Authors' Addresses	11

1. Introduction

Remote Attestation procedures (RATS, [RFC9334]) describe interactions between well-defined architectural constituents in support of Relying Parties that require an understanding about the trustworthiness of a remote peer. The identity of an Attester and its corresponding Attesting Environments play a vital role in RATS. A common way to refer to such an identity is the Authentication Secret ID as defined in the Reference Interaction Models for RATS [I-D.ietf-rats-reference-interaction-models]. The fact that every Attesting Environment can be uniquely identified in the context of the RATS architecture is not suitable for every application of remote attestation. Additional issues may arise when Personally identifiable information (PII) -- whether obfuscated or in clear text -- are included in attestation Evidence or even corresponding Attestation Results. This document illustrates how Direct Anonymous Attestation (DAA) can mitigate the issue of uniquely (re-)identifiable Attesting Environments. To accomplish that goal, the protocol entity DAA Issuer as described in [DAA] is introduced and its duties as well as its mappings with other RATS roles are specified.

2. Terminology

This document uses the following set of terms, roles, and concepts as defined in [RFC9334]: Attester, Verifier, Relying Party, Endorser, Conceptual Message, Evidence, Attestation Result, Attesting Environment.

Additionally, this document uses and adapts, as necessary, the following concepts and information elements as defined in [I-D.ietf-rats-reference-interaction-models]: Attester Identity, Authentication Secret, Authentication Secret ID

A PKIX Certificate is an X.509v3 format certificate as specified by [RFC5280].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Direct Anonymous Attestation

Two protocols as described in [DAA] are illustrated: the Join Protocol and the DAA-Signing Protocol. This section specifies the mapping of the protocol entity DAA Issuer described in [DAA] as an actor in the Join Protocol as well as an actor in the corresponding DAA-Signing Protocol to roles specified in the RATS Architecture.

In the Join Protocol, the protocol entity DAA Issuer takes on the RATS roles of Verifier and associated Relying Party. The mapping is illustrated in Figure 1.

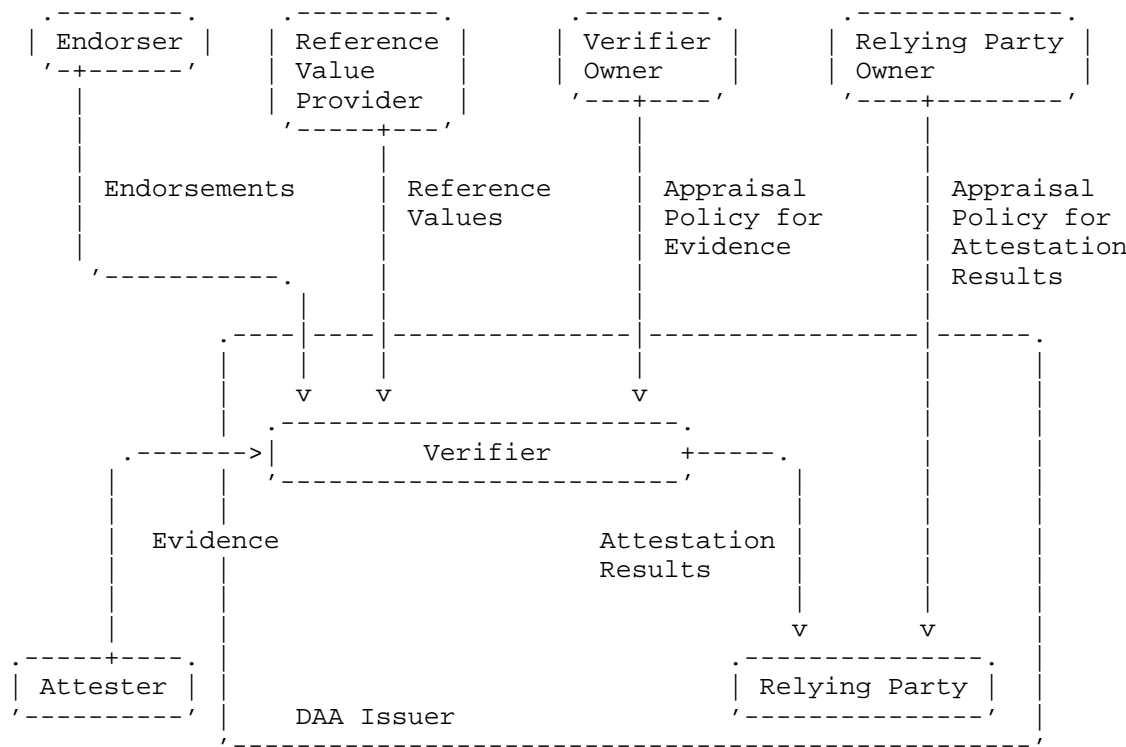


Figure 1: RATS Architecture for the Join Protocol

The Join Protocol is essentially an enrollment protocol that consumes Evidence from the Attester (therefore the mapping to the Verifier role). Corresponding Appraisal Policies for Evidence specific to the Join Protocol are used to produce Attestation Results to decide whether to issue a DAA credential to an Attester or not (therefore the mapping to the Relying Party role).

In the DAA-Signing Protocol, the RATS role Endorser is then taken on by the DAA Issuer protocol entity. The mapping is illustrated in Figure 2.

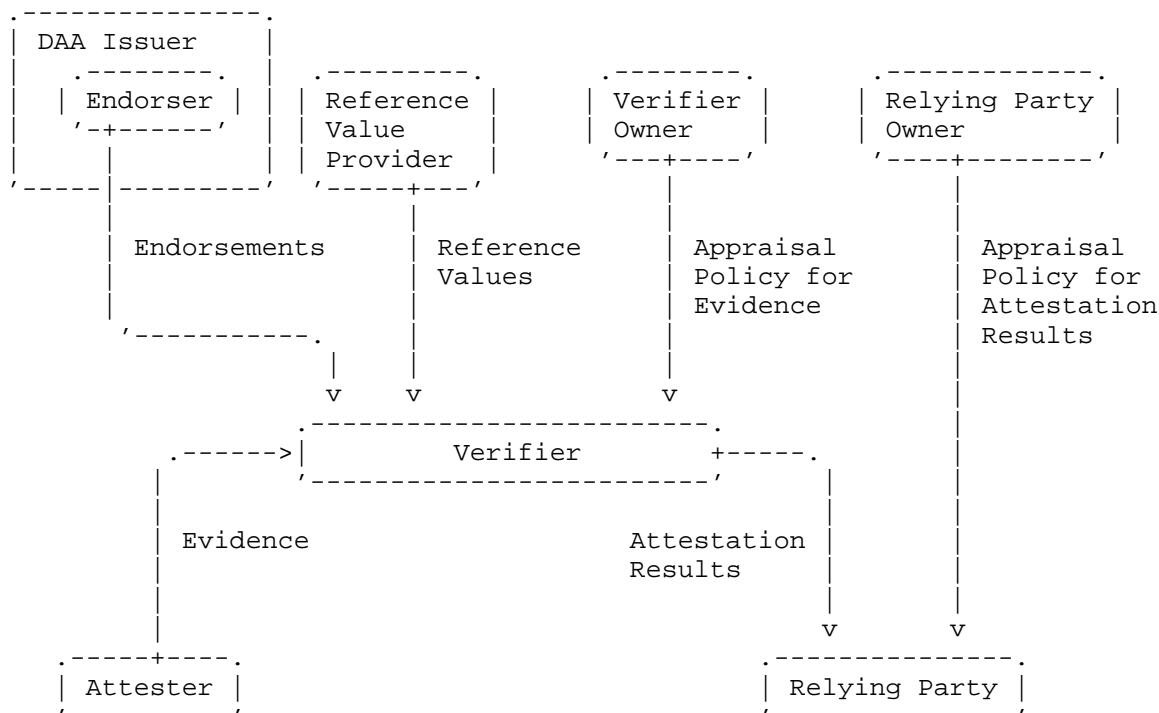


Figure 2: RATS Architecture for the DAA-Signing Protocol

The DAA Issuer acts as the Endorser for the Group Public Key that is used by the Verifier for the appraisal of evidence of anonymized Attesters that use the DAA credentials and associated key material to produce Evidence.

In consequence, DAA provides a signature scheme that allows the privacy of users that are associated with an Attester (e.g., its owner) to be maintained. Essentially, DAA can be seen as a group signature scheme with the feature that given a DAA signature no-one can find out who the signer is, i.e., the anonymity is not revocable. To be able to sign anonymously, an Attester has to obtain a credential from a DAA Issuer. The DAA Issuer uses a private/public key pair to generate credentials for a group of Attesters and makes the public key (in the form of a public key certificate) available to the Verifier in order to enable it to validate the Evidence received.

In order to support these DAA signatures, the DAA Issuer MUST associate a single key pair with a group of Attesters and use the same key pair when creating the credentials for all of the Attesters in this group. The DAA Issuer's group public key certificate replaces the individual Attester Identity documents during authenticity validation as a part of the appraisal of Evidence conducted by a Verifier. This is in contrast to intuition that there has to be a unique Attester Identity per device.

For DAA, the role of the Endorser is essentially the same, but it now provides Endorsements to the DAA Issuer rather than directly to the Verifier. These Endorsements enable the Attester to obtain a credential from the DAA Issuer.

4. DAA changes to the RATS Architecture

In order to enable the use of DAA, a new conceptual message, the Credential Request, is defined and a new role, the DAA Issuer role, is added to the roles defined in the RATS Architecture.

Credential Request: An Attester sends a Credential Request to the DAA Issuer to obtain a credential. This request contains information about the DAA key that the Attester will use to create evidence and, together with Attester endorsement information that is provided by the Endorser, to confirm that the request came from a valid Attester.

DAA Issuer: A RATS role that offers zero-knowledge proofs based on public-key certificates used for a group of Attesters (Group Public Keys) [DAA]. How this group of Attesters is defined is not specified here, but the group must be large enough for the necessary anonymity to be assured.

Effectively, these certificates share the semantics of Endorsements, with the following exceptions:

- * Upon receiving a Credential Request from an Attester, the associated group private key is used by the DAA Issuer to provide the Attester with a credential that it can use to convince the Verifier that its Evidence is valid. To keep their anonymity, the Attester randomizes this credential each time that it is used. Although the DAA Issuer knows the Attester Identity and can associate this with the credential issued, randomization ensures that the Attester's identity cannot be revealed to anyone, including the DAA Issuer.

- * The Verifier can use the DAA Issuer's group public key certificate, together with the randomized credential from the Attester, to confirm that the Evidence comes from a valid Attester without revealing the Attester's identity.
- * A credential is conveyed from a DAA Issuer to an Attester in combination with the conveyance of the group public key certificate from DAA Issuer to Verifier.

5. Additions to Remote Attestation principles

In order to ensure an appropriate conveyance of Evidence via interaction models in general, the following prerequisite considering Attester Identity MUST be in place to support the implementation of interaction models.

Attestation Evidence Authenticity: Attestation Evidence MUST be authentic.

In order to provide proofs of authenticity, Attestation Evidence SHOULD be cryptographically associated with an identity document that is a randomized DAA credential.

The following information element defines extensions for corresponding information elements defined in [I-D.ietf-rats-reference-interaction-models], which are vital to all types of reference interaction models. Varying from solution to solution, generic information elements can be either included in the scope of protocol messages (instantiating Conceptual Messages defined by the RATS architecture) or can be included in additional protocol parameters of protocols that facilitate the conveyance of RATS Conceptual Messages. Ultimately, the following information element is required by any kind of scalable remote attestation procedure using DAA with one of RATS's reference interaction models.

Attesting Environment IDs ('attEnvIDs'): _mandatory_

In DAA, the Attesting Environment's identity is not revealed to the Verifier. Attesting Environments MUST be issued with a credential by the DAA Issuer that is randomized and then used to anonymously confirm the validity of their Evidence. Corresponding Evidence is appraised using the DAA Issuer's group public key.

In DAA, Attesting Environment ID does not identify a unique Attesting Environment but is associated with a group of Attesting Environments. This is because an Attesting Environment should not be distinguishable and the DAA credential which represents the Attesting Environment is randomized each time it is used.

6. Implementation Status

Note to RFC Editor: Please remove this section as well as references to [BCP205] before AUTH48.

This section records the status of known implementations of the protocol defined by this specification at the time of posting of this Internet-Draft, and is based on a proposal described in [BCP205]. The description of implementations in this section is intended to assist the IETF in its decision processes in progressing drafts to RFCs. Please note that the listing of any individual implementation here does not imply endorsement by the IETF. Furthermore, no effort has been spent to verify the information presented here that was supplied by IETF contributors. This is not intended as, and must not be construed to be, a catalog of available implementations or their features. Readers are advised to note that other implementations may exist.

According to [BCP205], "this will allow reviewers and working groups to assign due consideration to documents that have the benefit of running code, which may serve as evidence of valuable experimentation and feedback that have made the implemented protocols more mature. It is up to the individual working groups to use this information as they see fit".

6.1. Implementer

The open-source implementation was initiated and is maintained by Ubitech.

6.2. Implementation Name

The open-source implementation is named "TPM Direct Anonymous Attestation (DAA) Library".

6.3. Implementation URL

The open-source implementation project resource can be located via: <https://github.com/ubitech/daa> (<https://github.com/ubitech/daa>)

6.4. Maturity

The code's level of maturity is considered to be "production".

6.5. Coverage and Version Compatibility

The current version ('ce85eb1') implements a C library and reference implementation of Direct Anonymous Attestation (DAA) targeting TPM 2.0-equipped platforms and the IBM TPM 2.0 simulator.

6.6. License

The Ubitech DAA project and all corresponding code and data maintained on GitHub are provided under the MIT license.

6.7. Implementation Dependencies

The implementation requires the use of the Trusted Computing Group (TCG) Trusted Software Stack (TSS), and an HSM interoperable with the Trusted Platform Module Library specifications, e.g., a Trusted Platform Module (TPM) 2.0 or equivalent implementation. The corresponding project resources (code and data) for Linux-based operating systems are maintained on GitHub at <https://github.com/tpm2-software/tpm2-tss/> (<https://github.com/tpm2-software/tpm2-tss/>).

6.8. Contact

Thanassis Giannetsos (agiannetsos@ubitech.eu)

7. Privacy Considerations

As outlined above, for DAA to provide privacy for the Attester, the DAA group must be large enough to stop the Verifier identifying the Attester.

Randomization of the DAA credential by the Attester means that collusion between the DAA Issuer and Verifier, will not give them any advantage when trying to identify the Attester.

For DAA, the Attestation Evidence conveyed to the Verifier MUST not uniquely identify the Attester. If the Attestation Evidence is unique to an Attester other cryptographic techniques can be used, for example, property based attestation [PBA].

8. Security Considerations

The anonymity property of DAA makes revocation difficult. Well known solutions include:

1. Rogue Attester revocation -- if an Attester's private key is compromised and known by the Verifier then any DAA signature from that Attester can be revoked.

2. EPID - Intel's Enhanced Privacy ID -- this requires the Attester to prove (as part of their Attestation) that their credential was not used to generate any signature in a signature revocation list.

There are no other special security considerations for DAA over and above those specified in the RATS architecture document [RFC9334].

9. Implementation Considerations

The new DAA Issuer role can be implemented in a number of ways, for example:

1. As a stand-alone service like a Certificate Authority, a Privacy CA.
2. As a part of the Attester's manufacture. The Endorser and the DAA Issuer could be the same entity and the manufacturer would then provide a certificate for the group public key to the Verifier.

10. References

10.1. Normative References

- [BCP205] Best Current Practice 205,
<<https://www.rfc-editor.org/info/bcp205>>.
At the time of writing, this BCP comprises the following:
- Sheffer, Y. and A. Farrel, "Improving Awareness of Running Code: The Implementation Status Section", BCP 205,
RFC 7942, DOI 10.17487/RFC7942, July 2016,
<<https://www.rfc-editor.org/info/rfc7942>>.
- [DAA] Brickell, E., Camenisch, J., and L. Chen, "Direct anonymous attestation", ACM, DOI 10.1145/1030083.1030103,
Proceedings of the 11th ACM conference on Computer and communications security pp. 132-145, October 2004,
<<https://doi.org/10.1145/1030083.1030103>>.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119,
DOI 10.17487/RFC2119, March 1997,
<<https://doi.org/10.17487/RFC2119>>.

- [RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <<https://doi.org/10.17487/RFC5280>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://doi.org/10.17487/RFC8174>>.

10.2. Informative References

- [I-D.ietf-rats-reference-interaction-models] Birkholz, H., Eckel, M., Pan, W., and E. Voit, "Reference Interaction Models for Remote Attestation Procedures", Work in Progress, Internet-Draft, draft-ietf-rats-reference-interaction-models-14, 7 July 2025, <<https://datatracker.ietf.org/doc/html/draft-ietf-rats-reference-interaction-models-14>>.
- [PBA] Chen, L., Lühr, H., Manulis, M., and A. Sadeghi, "Property-Based Attestation without a Trusted Third Party", Springer Berlin Heidelberg, DOI 10.1007/978-3-540-85886-7_3, ISBN ["9783540858843", "9783540858867"], Lecture Notes in Computer Science pp. 31-46, September 2008, <https://doi.org/10.1007/978-3-540-85886-7_3>.
- [RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedures (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <<https://doi.org/10.17487/RFC9334>>.

Authors' Addresses

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany
Email: henk.birkholz@ietf.contact

Christopher Newton
University of Surrey
Email: cn0016@surrey.ac.uk

Liqun Chen
University of Surrey
Email: liqun.chen@surrey.ac.uk

Thanassis Giannetsos
Ubitech
Email: agiannetsos@ubitech.eu

Dave Thaler
Microsoft
United States of America
Email: dthaler@microsoft.com