Network Working Group
Internet-Draft
Intended status: Informational
Expires: 14 November 2026

J. D. Hillier
Certisyn, Inc.

13 May 2026

Essential Eight Verified — A Cryptographic Verification Standard for the ACSC Essential Eight Maturity Model

draft-hillier-certisyn-essential-eight-verified-00

Abstract

This document specifies a verification standard for the cryptographic attestation of conformance to the Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model. It defines the Verification Reconciliation Object (VRO), the issuing-partner framework, the evidence categories required for each of the eight controls of the Essential Eight, the three maturity-attestation levels, and the cryptographic continuity requirements that together produce deterministic, independently reconstructable, auditor-grade attestations of cybersecurity posture. The standard sits beneath the ACSC Essential Eight Maturity Model and produces the verifiable artefact the model was designed to imply but does not deliver.

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 14 November 2026.

Copyright Notice

Table of Contents

1. Introduction

The ACSC Essential Eight Maturity Model [ACSC-E8] is the de facto baseline for cybersecurity posture across Australian government suppliers, regulated industries, and critical infrastructure. It is referenced in procurement criteria, regulatory expectations, insurance underwriting questionnaires, and intergovernmental supplier assurance frameworks.

The Essential Eight Maturity Model is, however, a self-attested instrument. The ACSC publishes the framework but does not maintain a certification regime, an auditor accreditation scheme, or a verification artefact. Suppliers asserting Essential Eight alignment produce policy documents and internal self-assessments. Buyers asserting Essential Eight reliance accept those self-assessments at face value or commission ad-hoc third-party reviews that are not interoperable across engagements.

This document closes that gap. It defines the verification artefact, the issuing-partner framework, the evidence requirements, the maturity attestation methodology, and the cryptographic continuity requirements that together produce a deterministic, auditor-grade Essential Eight attestation.

This document does not replace the ACSC Maturity Model. It sits beneath the model and produces the artefact the model was designed to imply but does not deliver. Where this document and the ACSC Maturity Model conflict on operational content, the ACSC Maturity Model prevails.

2. Conventions and Definitions

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.

For the purposes of this document, the following definitions apply.

Subject Entity: The organisation whose Essential Eight conformance is the subject of verification.

Verification Reconciliation Object (VRO): The deterministic, cryptographically anchored output of a conforming Essential Eight attestation under this standard.

Issuing Partner: A counterparty designated by the protocol operator to act as a co-issuer of VROs under this standard within a defined market or scope.

Attestation Period: The contiguous time interval over which a VRO asserts conformance, bounded by an Anchor Event at each terminus.

Anchor Event: The cryptographic operation that binds a VRO to an immutable public settlement layer at issuance and at supersession.

Maturity Level: One of three levels (One, Two, Three) defined in the ACSC Essential Eight Maturity Model, against which conformance is asserted.

Conformance Claim: An assertion by the Subject Entity, made within a VRO, that operational practice meets the requirements of a stated Maturity Level for a specified set of Essential Eight controls.

Evidence Artefact: Any document, telemetry record, configuration snapshot, log extract, or attestation produced in support of a Conformance Claim.

Supersession: The lifecycle event by which a new VRO replaces a prior VRO in the chain of attestation for a Subject Entity.

3. Architectural Overview

Conforming attestations under this standard are produced by a verification infrastructure organised as five architectural components. Internal design, scoring methodology, and calibration logic are not in scope for this document and are governed by the protocol operator’s intellectual property framework.

The Evidence Ingestion and Normalization Layer accepts Evidence Artefacts from Subject Entity systems and produces canonical inputs for downstream reconciliation.

The Reconciliation Confidence Engine reconciles Conformance Claims against normalised evidence and produces a deterministic reconciliation output.

The Verification State Machine maintains the lifecycle state of each VRO through intake, evidence ingestion, reconciliation, anchoring, issuance, supersession, and revocation.

Entity Graph Propagation propagates verification state across related entities where continuity is in scope.

The Attestation Protocol produces the final VRO, performs the Anchor Event, registers the artefact in the public attestation registry, and binds the issuing-partner identity to the artefact.

Conforming attestations are deterministic. Given the same Conformance Claims and the same Evidence Artefacts processed through the same Attestation Protocol version, the same VRO SHALL be produced.

4. Essential Eight Verification Requirements

The following subsections specify, for each of the eight controls in the ACSC Essential Eight Maturity Model, the Subject Claim that is the object of verification, the categories of Evidence Artefact that SHALL be ingested and reconciled, the verification expectation applied by the Reconciliation Confidence Engine, and the anchoring requirement that binds the resulting VRO to the public settlement layer.

4.1. Control 1: Application control

Subject Claim: The Subject Entity restricts execution of unauthorised applications across all in-scope endpoints, consistent with the asserted Maturity Level.

Evidence Categories: Application allow-list policy artefact; endpoint enforcement telemetry; deviation log; periodic review records; exception register.

Verification Expectation: Reconciliation of declared allow-list against enforcement evidence with continuity across the Attestation Period; exception cases reconciled against the exception register.

Anchor Requirement: Each issued VRO under this control SHALL be anchored at Attestation Period start and end. Mid-period deviations producing a state change require a supersession anchor.

4.2. Control 2: Patch applications

Subject Claim: The Subject Entity applies vendor-supplied security patches to in-scope applications within timeframes consistent with the asserted Maturity Level.

Evidence Categories: Application inventory; patch availability metadata; patch deployment telemetry; vulnerability scan output; exceptions and compensating-control register.

Verification Expectation: Temporal reconciliation of patch availability date against deployment date across the in-scope application population. Exceptions reconciled against compensating controls evidence.

Anchor Requirement: Anchored at Attestation Period start, end, and any material change in patch posture.

4.3. Control 3: Configure Microsoft Office macro settings

Subject Claim: The Subject Entity has configured Microsoft Office macro settings consistent with ACSC guidance and the asserted Maturity Level, and operates an audit cadence to detect drift.

Evidence Categories: Group Policy artefacts or equivalent configuration management evidence; endpoint configuration snapshots; macro source attestation where macros are permitted; exception register.

Verification Expectation: Reconciliation of declared configuration against endpoint snapshots; reconciliation of permitted macro inventory against signed-source attestations.

Anchor Requirement: Anchored at issuance; supersession on any change to macro policy or scope of permitted use.

4.4. Control 4: User application hardening

Subject Claim: The Subject Entity has hardened user-facing applications consistent with ACSC guidance for the asserted Maturity Level.

Evidence Categories: Hardening policy artefact; endpoint configuration baseline; periodic configuration audit output; exception register.

Verification Expectation: Reconciliation of declared hardening baseline against measured endpoint state. Drift items reconciled against remediation evidence.

Anchor Requirement: Anchored at issuance; supersession on baseline change or material drift remediation.

4.5. Control 5: Restrict administrative privileges

Subject Claim: The Subject Entity restricts the assignment and use of administrative privileges consistent with the asserted Maturity Level.

Evidence Categories: Privilege assignment register; access review records; privileged session monitoring telemetry; account separation evidence; just-in-time elevation telemetry where in scope.

Verification Expectation: Reconciliation of declared privilege model

against assignment register; reconciliation of access reviews against scheduled cadence; reconciliation of session monitoring evidence against asserted controls.

Anchor Requirement: Anchored at issuance and at the conclusion of each scheduled access review cycle within the Attestation Period.

4.6. Control 6: Patch operating systems

Subject Claim: The Subject Entity applies vendor-supplied security patches to operating systems within timeframes consistent with the asserted Maturity Level.

Evidence Categories: Operating-system inventory; patch availability metadata; patch deployment telemetry; vulnerability scan output; compensating-control register.

Verification Expectation: Temporal reconciliation of patch availability date against deployment date across the in-scope operating-system population.

Anchor Requirement: Anchored at Attestation Period start, end, and any material change in patch posture.

4.7. Control 7: Multi-factor authentication

Subject Claim: The Subject Entity enforces multi-factor authentication consistent with the population and access-context scope required at the asserted Maturity Level.

Evidence Categories: MFA enrolment register; identity-provider telemetry; coverage report by user population and access context; phishing-resistance attestation where applicable; exception register.

Verification Expectation: Reconciliation of declared MFA scope against identity-provider telemetry; reconciliation of asserted phishing-resistance properties against enrolment evidence.

Anchor Requirement: Anchored at issuance and at each material change in MFA scope, factor type, or enforcement state.

4.8. Control 8: Regular backups

Subject Claim: The Subject Entity maintains regular backups of important data, software, and configuration consistent with the asserted Maturity Level, and validates recoverability.

Evidence Categories: Backup policy artefact; backup execution telemetry; recovery test records; immutability evidence for the asserted retention period; access-control evidence for backup systems.

Verification Expectation: Reconciliation of declared backup cadence against execution telemetry; reconciliation of asserted immutability properties against backup-store configuration evidence; reconciliation of recovery test cadence and outcomes against declared schedule.

Anchor Requirement: Anchored at issuance and at each completed recovery validation cycle within the Attestation Period.

5. Maturity Level Attestation

The ACSC Essential Eight Maturity Model defines three Maturity Levels — One, Two, and Three — each progressively more rigorous in operational expectation, scope, and adversarial threat model. A conforming VRO under this standard SHALL attest a Maturity Level for each of the eight controls. Different controls MAY attest at different Maturity Levels within a single VRO; the overall VRO attestation is the minimum Maturity Level attested across the eight controls unless otherwise asserted.

Maturity Level One verification requirements reflect the operational expectations defined by the ACSC for Level One: protection against adversaries opportunistically leveraging publicly available exploit tradecraft. Evidence requirements emphasise the existence of declared controls and basic enforcement evidence over an Attestation Period of at least three (3) consecutive months.

Maturity Level Two verification requirements reflect the ACSC’s Level Two expectation of protection against adversaries operating with a moderate level of capability and investment. Evidence requirements add depth of telemetry, periodic review evidence, and exception-handling discipline over an Attestation Period of at least six (6) consecutive months.

Maturity Level Three verification requirements reflect the ACSC’s Level Three expectation of protection against adversaries with significant capability, investment, and willingness to invest in tailored tradecraft. Evidence requirements add continuity, defence-in-depth evidence, and adversarial-resistance attestations over an Attestation Period of at least twelve (12) consecutive months.

A Subject Entity that progresses from one Maturity Level to a higher level for any control SHALL be issued a superseding VRO that records the progression, the date of progression, and the Anchor Event binding the new attestation. The prior VRO is not deleted; it is preserved in the chain and marked as superseded.

6. Verification Reconciliation Object (VRO)

A conforming VRO under this standard SHALL contain, at minimum, the following content elements:

* Subject Entity identifier and metadata sufficient to establish identity under the relevant jurisdiction.

* Attestation Period start and end timestamps.

* Maturity Level attested for each of the eight Essential Eight controls.

* Conformance Claims as asserted by the Subject Entity.

* Evidence categories ingested and the reconciliation outcome for each.

* Issuing Partner identity and seat designation.

* Anchor Event identifiers binding the VRO to the public settlement layer.

* Verification State Machine state at issuance.

* Supersession chain reference, where this VRO supersedes a prior VRO.

* Conformance statement of this standard, version 1.0.

A VRO MAY be issued only by a designated Issuing Partner. Issuing Partner identity is bound to the VRO at the Anchor Event and is independently verifiable through the public attestation registry.

A VRO MAY be revoked by the Issuing Partner upon determination of material non-conformance, evidence falsification, or other circumstances rendering the original attestation unreliable. Revocation does not delete the VRO; it records a revocation state, the revocation reason class, and the Anchor Event binding the revocation to the public settlement layer. Supersession is the ordinary lifecycle event by which a current VRO is replaced; revocation is reserved for circumstances of attestation failure.

Each issued VRO SHALL be registered in the public attestation registry. Registry entries SHALL be queryable by Subject Entity identifier, Issuing Partner, Anchor Event, and supersession chain.

7. Issuing Partner Requirements

An organisation seeking designation as an Issuing Partner under this standard SHALL demonstrate, at minimum:

* Operational capacity to assess Essential Eight conformance across the eight controls at the Maturity Level for which issuance is sought.

* Demonstrable competence in the relevant subject matter.

* Independence from the Subject Entity at the engagement level, with declared conflicts of interest disclosed and managed.

* Adherence to the protocol operator’s Partner Code of Conduct.

* Acceptance of the Designation Schedule terms applicable to the relevant market and seat.

An Issuing Partner SHALL NOT, for a given Subject Entity engagement, simultaneously act as the implementing vendor, system integrator, or operator of the controls being verified. Where an Issuing Partner has performed implementing work for a Subject Entity, a defined cooling-off interval and an independence declaration SHALL be observed before that Issuing Partner may issue a VRO for the same Subject Entity.

8. Cryptographic Continuity Requirements

Each VRO SHALL be cryptographically anchored to an immutable public settlement layer at the Anchor Event. The hash committed at the Anchor Event SHALL be a one-way function of the VRO content, Issuing Partner identity, and timestamp, computed under a digest algorithm of at least 256-bit strength.

A VRO issued under this standard SHALL remain a conforming artefact across regulatory regime changes occurring within or after the Attestation Period. Conformance to this standard is bound to the standard version at issuance; subsequent standard versions do not retroactively alter the conformance state of previously issued VROs.

The Anchor Event binding SHALL remain independently verifiable in the event of the protocol operator ceasing to operate the verification infrastructure. The public settlement layer is selected on the criterion that no single private operator can extinguish the binding.

9. Standards Alignment

This standard is interoperable with adjacent international and national standards. Conforming VROs MAY be referenced within the audit and certification artefacts produced under the following frameworks.

ISO/IEC 27001:2022 [ISO27001]: Essential Eight controls map to specific Annex A controls. Conforming VROs MAY be cited as evidence of operational implementation of those Annex A controls.

ISO/IEC 27002:2022 [ISO27002]: Implementation guidance for the Annex A controls cited above is consistent with the evidence categories specified herein.

SOC 2 Trust Services Criteria: Conforming VROs MAY be cited within SOC 2 reports as evidence of controls operating effectively over the relevant Attestation Period.

ACSC Essential Eight Maturity Model [ACSC-E8] remains authoritative for the operational definition of each control. This standard adds a verification layer without redefining operational content.

10. Conformance

An attestation artefact MAY claim conformance to this standard if and only if it satisfies every requirement specified in this document. Partial conformance is not recognised. Variant conformance to a subset of controls without the full Essential Eight scope is not recognised.

The public attestation registry constitutes the authoritative record of issued VROs. Inclusion in the registry is necessary for conformance recognition; exclusion from the registry, regardless of any other instrument, precludes recognition under this standard.

11. IANA Considerations

This document has no IANA actions.

12. Security Considerations

The integrity of an attestation under this standard depends on the independence of the issuing rail, the determinism of the reconciliation engine, and the survivability of the cryptographic anchor.

Issuing Partners are required to be independent from the Subject Entity at the engagement level. Operators of this standard SHOULD audit independence declarations periodically.

The Anchor Event is the binding mechanism. Implementations SHOULD use a digest algorithm of at least 256-bit strength and SHOULD select a public settlement layer with no single private operator capable of extinguishing the binding.

Revocation procedures defined herein prevent silent acceptance of attestations whose underlying evidence has been later determined to be falsified or materially incomplete.

This standard does not address physical security of the Subject Entity, regulatory compliance beyond Essential Eight scope, or the correctness of the ACSC Maturity Model itself.

13. References

13.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

13.2. Informative References

[ACSC-E8] Centre, A. C. S., "Essential Eight Maturity Model", 2024, <https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/essential-eight/essential-eight-maturity-model>.

[ISO27001] Standardization, I. O. for., "Information security, cybersecurity and privacy protection — Information security management systems — Requirements", ISO/IEC 27001:2022, 2022.

[ISO27002] Standardization, I. O. for., "Information security, cybersecurity and privacy protection — Information security controls", ISO/IEC 27002:2022, 2022.

Acknowledgments

The author thanks the ANZ Founding Partner cohort for early review of this draft.

Author’s Address

Joel David Hillier
Certisyn, Inc.
Email: jhillier@certisyn.com
URI: https://certisyn.com/