Network Working Group J. Richer, Ed.

Internet-Draft Bespoke Engineering

Intended status: Standards Track L. Johansson

Expires: March 7, 2016 Swedish University Network

 September 4, 2015

 Vectors of Trust

 draft-richer-vectors-of-trust-01

Abstract

 This document defines a mechanism for describing and signaling

 several aspects that are used to calculate trust placed in a digital

 identity transaction.

Requirements Language

 The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

 "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this

 document are to be interpreted as described in RFC 2119 [RFC2119].

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 http://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 March 7, 2016.

Copyright Notice

 Copyright (c) 2015 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

 (http://trustee.ietf.org/license-info) in effect on the date of

 publication of this document. Please review these documents

Richer & Johansson Expires March 7, 2016 [Page 1]

Internet-Draft vectors-of-trust September 2015

 carefully, as they describe your rights and restrictions with respect

 to this document. Code Components extracted from this document must

 include Simplified BSD License text as described in Section 4.e of

 the Trust Legal Provisions and are provided without warranty as

 described in the Simplified BSD License.

Table of Contents

 1. Introduction . . . . . . . . . . . . . . . . . . . . . . . . 2

 1.1. Terminology . . . . . . . . . . . . . . . . . . . . . . . 3

 1.2. An Identity Model . . . . . . . . . . . . . . . . . . . . 4

 1.3. Component Architecture . . . . . . . . . . . . . . . . . 5

 2. Core Components . . . . . . . . . . . . . . . . . . . . . . . 5

 2.1. Identity Proofing . . . . . . . . . . . . . . . . . . . . 6

 2.2. Primary Credential Usage . . . . . . . . . . . . . . . . 6

 2.3. Primary Credential Management . . . . . . . . . . . . . . 6

 2.4. Assertion Presentation . . . . . . . . . . . . . . . . . 6

 3. Vectors of Trust Inititial Component Definitions . . . . . . 7

 4. Communicating Vector Values to RPs . . . . . . . . . . . . . 8

 4.1. On the Wire Representation . . . . . . . . . . . . . . . 8

 4.2. In OpenID Connect . . . . . . . . . . . . . . . . . . . . 9

 4.3. In SAML . . . . . . . . . . . . . . . . . . . . . . . . . 9

 5. Requesting Vector Values . . . . . . . . . . . . . . . . . . 10

 5.1. In OpenID Connect . . . . . . . . . . . . . . . . . . . . 10

 6. Discovery and Verification . . . . . . . . . . . . . . . . . 10

 6.1. Trustmark . . . . . . . . . . . . . . . . . . . . . . . . 10

 6.2. Discovery . . . . . . . . . . . . . . . . . . . . . . . . 12

 7. Acknowledgements . . . . . . . . . . . . . . . . . . . . . . 12

 8. IANA Considerations . . . . . . . . . . . . . . . . . . . . . 12

 8.1. Vector Of Trust Components Registry . . . . . . . . . . . 12

 8.2. Additions to JWT Claims Registry . . . . . . . . . . . . 13

 9. Security Considerations . . . . . . . . . . . . . . . . . . . 13

 10. Privacy Considerations . . . . . . . . . . . . . . . . . . . 13

 11. References . . . . . . . . . . . . . . . . . . . . . . . . . 14

 11.1. Normative References . . . . . . . . . . . . . . . . . . 14

 11.2. Informative References . . . . . . . . . . . . . . . . . 14

 Appendix A. Document History . . . . . . . . . . . . . . . . . . 14

 Appendix B. Example Extension . . . . . . . . . . . . . . . . . 15

 Authors' Addresses . . . . . . . . . . . . . . . . . . . . . . . 15

1. Introduction

 This document defines a mechanism for measuring

 several aspects of digital identity transactions that are used to

 determine a level of trust in that transaction. In the past, there

 have been two extremes of communicating authentication transaction

 information. On one end, all attributes are communicated with full

 provenance and associated trust markings. This approach seeks to

Richer & Johansson Expires March 7, 2016 [Page 2]

Internet-Draft vectors-of-trust September 2015

 create a fully distributed attribute system to support

 security functions like attribute based access control (ABAC). These attributes

 can be used to describe the end user, the identity provider, the

 relying party, or even the transaction itself. While the information

 that can be expressed in this model is incredible, the complexity of

 such a system is often prohibitive to align across security domains,

 especially to relying parties needing to process the sea of disparate

 attributes.

 At the other extreme there are systems that collapse all of the

 attributes and aspects into a single scalar value that communicates,

 in sum, how much a transaction can be trusted. The NIST special

 publication 800-63 [SP-800-63] defines a linear scale Level of

 Assurance (LoA) measure that combines multiple attributes about an

 identity transaction into a single measure of the level of trust a

 relying party should place on an identity transaction. Even though

 this definition was originally made for a specific government use

 cases, the LoA scale appeared to be applicable with a wide variety of

 authentication use cases. This has led to a proliferation of

 incompatible interpretations of the same scale in different trust

 frameworks, preventing interoperability between these frameworks in

 spite of their common measurement. Since identity proofing strength

 increases linearly along with credential strength in the LoA scale,

 this scale is too limited for describing many valid and useful forms

 of an identity transaction. For example, an anonymously assigned

 hardware token can be used in cases where the real world identity of

 the subject cannot be known, for privacy reasons, but the credential

 itself can be highly trusted.

 This work seeks to find a balance between these two extremes by

 creating a data model that combines attributes of the user and

 aspects of the authentication context into several values that can be

 communicated together. This approach is both coarser grained than

 the distributed attributes model and finer grained than the single

 value model, with the hope that it is a viable balance of

 expressivity and processability. Importantly, these three levels of

 granularity can be mapped to each other. The information of several

 attributes can be folded into a vector component, while the vector

 itself can be folded into an assurance category. As such, the

 vectors of trust seeks to complement, not replace, these other

 identity and trust mechanisms.

1.1. Terminology

 Identity Provider (IdP) A system that manages identity information

 and is able to assert this information across the network through

 an identity API.

Richer & Johansson Expires March 7, 2016 [Page 3]

Internet-Draft vectors-of-trust September 2015

 Identity Subject The person (user) engaging in the identity

 transaction, being identified by the identity provider and

 identified to the relying party.

 Primary Credential The credential used by the identity subject to

 authenticate to the identity provider.

 Federated Credential The assertion presented by the IdP to the RP

 across the network to authenticate the user.

 Relying Party (RP) A system that consumes identity information from

 an IdP for the purposes of authenticating the user.

 Trust Framework A document containing business rules and legal

 clauses that defines how different parties in an identity

 transaction may act.

 Trustmark A verifiable attestation that a party has proved to follow

 the constraints of a trust framework.

 Trustmark Provider A system that issues and provides verification

 for trustmarks.

 Vector A multi-part data structure, used here for conveying

 information about an authentication transaction.

 Vector Component One of several constituent parts that make up a

 vector.

1.2. An Identity Model

 This document assumes the following model for identity. Entities in the model include identity subject, identity provider, relying party, etc.

 The identity subject (aka user) is associated with an identity

 provider which acts as a trusted 3rd party on behalf of the user with

 regard to a relying party by making identity assertions about the

 user to the relying party.

 The real-world person represented by the identity subject is in

 possession of a primary credential bound to the identity subject by

 identity provider (or an agent thereof) in such a way that the

 binding between the credential and the real-world user is a

 representation of the identity proofing process performed by the the

 identity provider (or an agent thereof) to verify the identity of the

 real-world person.

Richer & Johansson Expires March 7, 2016 [Page 4]

Internet-Draft vectors-of-trust September 2015

1.3. Component Architecture

 The term Vectors of Trust is based on the mathematical construct of a

 Vector, which is defined as an item composed of multiple independent

 scalar values. A vector is a set of coordinates that specifies a

 point in a (multi-dimensional) Cartesian coordinate space. The

 reader is encouraged to think of a vector of trust as a point in a

 coordinate system, in the simples form (described below) a 3

 dimensional space that is intended to be a recognizable, if somewhat

 elided, model of identity subject trust.

 An important goal for this work is to balance the need for simplicity

 (particularly on the part of the relying party) with the need for

 expressiveness. As such, this vector construct is designed to be

 composable and extensible

 All components of the vector construct MUST be orthogonal in the

 sense that no aspect of a component overlap an aspect of another

 component.

 The values assigned to each component of a vector is sometimes

 written as an ordinal number (e.g. an integer) but MUST NOT be

 assumed as having inherent ordinal properties when compared to the

 same or other components in the vector space. In other words, 1 is

 different from 2, but it is dangerous to assume that 2 is always

 "more" (better) than 1.

2. Core Components

 This specification defines four orthogonal components: identity

 proofing, primary credential usage, primary credential management, and

 assertion presentation. These dimensions MUST be evaluated in the

 context of a trust framework and SHOULD be combined with other

 information when making a trust and authorization decision.

 This specification also defines values for each component to be used

 in the absence of a more specific trust framework. It is expected

 that trust frameworks will provide context, semantics, and mapping to

 legal statutes and business rules for each value in each component.

 Consequently, a particular vector value can only be compared with

 vectors defined in the same context. The RP MUST understand and take

 into account the trust framework context in which a vector is being

 expressed in order for it to be processed securely.

 It is anticipated that trust frameworks will also define additional

 components using the component registry established in Section 8.

Richer & Johansson Expires March 7, 2016 [Page 5]

Internet-Draft vectors-of-trust September 2015

 Each component is identified by a demarcator consisting of a single

 case-sensitive ASCII character in the range [A-Za-z]. A value for a

 given component is defined by its demarcator character followed by a

 single case-sensitive ASCII character in the range [0-9A-Za-z].

2.1. Identity Proofing

 The Identity Proofing dimension defines, overall, how strongly the

 set of identity attributes have been verified and vetted, and how

 strongly they are tied to a particular credential set. In other

 words, this dimension describes how likely it is that a given digital

 identity corresponds to a particular (real-world) identity subject.

 This dimension SHALL be represented by the "P" demarcator and a

 single-character level value, such as "P1", "P2", etc.

2.2. Primary Credential Usage

 The primary credential usage dimension defines how strongly the

 primary credential can be verified by the IdP. In other words, and

 how easily that credential could be spoofed or stolen.

 This dimension SHALL be represented by the "C" demarcator and a

 single-character level value, such as "C1", "C2", etc. Multiple

 credential usage factors MAY be communicated simultaneously, such as

 when Multi-Factor Authentication is used.

2.3. Primary Credential Management

 The primary credential management dimension conveys information about

 the expected lifecycle of the primary credential in use, including

 its binding, rotation, and revocation. This component defines how

 strongly the primary credential can be trusted to be presented by the

 party represented by the credential based on knowledge of the

 management of the credentials at the IdP. In other words, this

 dimension describes how likely it is that the right person is

 presenting the credential to the identity provider.

 This dimension SHALL be represented by the "M" demarcator and a

 single-character level value, such as "M1", "M2", etc.

2.4. Assertion Presentation

 The Assertion Presentation dimension defines how well the given

 digital identity can be communicated across the network without

 information leaking to unintended parties, and without spoofing. In

 other words, this dimension describes how likely it is that a given

 digital identity asserted was actually asserted by a given identity

Richer & Johansson Expires March 7, 2016 [Page 6]

Internet-Draft vectors-of-trust September 2015

 provider for a given transaction. While this information is largely

 already known by the RP by the nature of processing an identity

 assertion, this dimension is still useful when the RP requests a

 login (Section 5) and when describing the capabilities of an IdP

 (Section 6.2).

 This dimension SHALL be represented by the "A" demarcator and a level

 value, such as "A1", "A2", etc.

3. Vectors of Trust Initial Component Definitions

 This specification defines the following general-purpose component

 definitions, which MAY be used when a more specific set is

 unavailable. These component values are referenced in a trustmark

 definition defined by [[ this document URL ]].

 P0 No proofing is done, data is not guaranteed to be persistent

 across sessions

 P1 Attributes are self-asserted but consistent over time, potentially

 pseudonymous

 P2 Identity has been proofed either in person or remotely using

 trusted mechanisms (such as social proofing)

 P3 There is a binding relationship between the identity provider and

 the identified party (such as signed/notarized documents,

 employment records)

 C0 No credential is used / anonymous public service / simple session

 cookies (with nothing else)

 C1 Known device

 C2 Shared secret such as a username and password combination

 C3 Cryptographic proof of key possession using shared key

 C4 Cryptographic proof of key possession using asymmetric key

 C5 Sealed hardware token / trusted biometric / TPM-backed keys

 M0 Self-asserted credentials

 M1 Remote issuance and rotation / use of backup recover credentials

 (such as email verification) / deletion on user request

Richer & Johansson Expires March 7, 2016 [Page 7]

Internet-Draft vectors-of-trust September 2015

 M2 Full proofing required for each issuance and rotation / revocation

 on suspicious activity

 A0 No protection / unsigned bearer identifier (such as a session

 cookie)

 A1 Signed and verifiable token, passed through the browser

 A2 Signed and verifiable token, passed through a back channel

 A3 Token encrypted to the relying parties’ key and audience protected

4. Communicating Vector Values to RPs

 All four of these dimensions (and others, as they are defined in

 extension work) MUST be combined into a single vector that can be

 communicated across the wire unbroken. All vector components MUST be

 individually available, MUST NOT be "collapsed" into a single value

 without also presenting the constituent dimensions as well.

 When communicating the vectors across the wire, they MUST be

 protected in transit and MUST signed by the asserting authority (such

 as the IdP).

4.1. On the Wire Representation

 The vector MUST be represented as a period-separated ('.') list of

 vector components, with no specific order. A vector component type

 MAY occur multiple times within a single vector, with each component

 separated by periods. Multiple values for a component are considered

 an AND of the values. A single value of a vector component MUST NOT

 occur more than once in a single vector. In order to simplify

 processing by RPs, it is RECOMMENDED that trust framework definitions

 carefully define component values such that they are mutually

 exclusive or subsumptive in order to avoid repeated vector components

 where possible.

 Vector components MAY be omitted from a vector. No holding space is

 left for an omitted vector component. If a vector component is

 omitted, the IdP is making no claim for that category.

 For example, the vector value "P1.C3.A2" translates to pseudonymous,

 proof of shared key, signed back-channel verified token in the

 context of this specification's definitions (Section 3).

 Vector values MUST be communicated alongside of a trustmark

 definition to give the component’s context. A vector value without

 context is unprocessable.

Richer & Johansson Expires March 7, 2016 [Page 8]

Internet-Draft vectors-of-trust September 2015

4.2. In OpenID Connect

 In OpenID Connect [OpenID], the IdP MUST send the vector value as a

 string with the "vot" (vector of trust) claim in the ID token. The

 trustmark (Section 6.1) that applies to this vector MUST be sent as

 an HTTPS URL in the "vtm" (vector trust mark) claim to provide

 context to the vector.

 For example:

 {

 "iss": "https://idp.example.com/",

 "sub": "jondoe1234",

 "vot": "P1.C3.A2",

 "vtm": "https://trustmark.example.org/trustmark/idp.example.com"

 }

4.3. In SAML

 In SAML a VoT vector is communicated as an

 AuthenticationContextClassRef, a sample definition of which might

 look something like this:

 <?xml version="1.0" encoding="UTF-8"?>

 <xs:schema

 targetNamespace="urn:x-vot:P1:C3:A2"

 xmlns:xs="http://www.w3.org/2001/XMLSchema"

 xmlns="urn:x-vot:P1.C3.A2"

 finalDefault="extension"

 blockDefault="substitution"

 version="2.0">

 <xs:redefine

 schemaLocation="saml-schema-authn-context-loa-profile.xsd"/>

 <xs:annotation>

 <xs:documentation>VoT vector P1.C3.A2</xs:documentation>

 </xs:annotation>

 <xs:complexType name="GoverningAgreementRefType">

 <xs:complexContent>

 <xs:restriction base="GoverningAgreementRefType">

 <xs:attribute name="governingAgreementRef"

 type="xs:anyURI"

 fixed="draft-ietf-vot-this-document-00.txt"

 use="required"/>

 </xs:restriction>

 </xs:complexContent>

 </xs:complexType>

 </xs:redefine>

 </xs:schema>

Richer & Johansson Expires March 7, 2016 [Page 9]

Internet-Draft vectors-of-trust September 2015

5. Requesting Vector Values

 In some identity protocols, the RP can request that particular

 attributes be applied to a given identity transaction.

5.1. In OpenID Connect

 In OpenID Connect [OpenID], the client can request a set of

 acceptable VoT values with the "vtr" (vector of trust request) claim

 request as part of the Request Object. The value of this field is an

 array of JSON strings, each string identifying an acceptable set of

 vector components. The components within each vector are ANDed

 together while the individual vector strings are ORed together.

 Vector request values MAY omit components, indicating that any value

 is acceptable.

 {

 "vtr": ["P1.C2.C3.A2", "C5.A2"]

 }

6. Discovery and Verification

6.1. Trustmark

 When an RP receives a specific vector from an IdP, it needs to make a

 decision to trust the vector within a specific context. A trust

 framework can provide such a context, allowing legal and business

 rules to give weight to an IdP's claims. A trustmark is a verifiable

 claim to conform to a specific component of a trust framework, such

 as a verified identity provider. The trustmark conveys the root of

 trustworthiness about the claims and assertions made by the IdP.

 The trustmark MUST be available from an HTTPS URL served by the trust

 framework provider. The contents of this URL are a JSON [RFC7159]

 document with the following fields:

 idp The issuer URL of the identity provider that this trustmark

 pertains to. This MUST match the corresponding issuer claim in

 the identity token, such as the OpenID Connect "iss" field. This

 MUST be an HTTPS URL.

 trustmark\_provider The issuer URL of the trustmark provider that

 issues this trustmark. The URL that a trustmark is fetched from

 MUST start with the "iss" URL in this field. This MUST be an

 HTTPS URL.

 P Array of strings containing identity proofing values for which the

 identity provider has been assessed and approved

Richer & Johansson Expires March 7, 2016 [Page 10]

Internet-Draft vectors-of-trust September 2015

 C Array of strings containing primary credential usage values for

 which the identity provider has been assessed and approved

 M Array of strings containing primary credential management values

 for which the identitity provider has been assessed and approved

 A Array of strings containing assertion strength values for which

 the identity provider has been assessed and approved

 Additional vector component values MUST be listed in a similar

 fashion using their demarcator.

 For example, the following trustmark provided by the

 trustmark.example.org organization applies to the idp.example.org

 identity provider:

 {

 "idp": "https://idp.example.org/",

 "trustmark\_provider": "https://trustmark.example.org/",

 "P": ["P0", "P1"],

 "C": ["C1", "C2", "C3"],

 "M": ["M2"],

 "A": ["C2", "C3"]

 }

 A client wishing to check the claims made by an IdP can fetch the

 information from the trustmark provider about what claims the IdP is

 allowed to make in the first place and process them accordingly.

 The means by which the RP decides which trustmark providers it trusts

 is out of scope for this specification and is generally configured

 out of band.

 Though most trust frameworks will provide a third-party independent

 verification service for components, an IdP MAY host its own

 trustmark. For example, a self-hosted trustmark would look like:

 {

 "idp": "https://idp.example.org/",

 "trustmark\_provider": "https://idp.example.org/",

 "P": ["C0", "C1"],

 "C": ["C1", "C2", "C3"],

 "M": ["M2"],

 "A": ["C2", "C3"]

 }

Richer & Johansson Expires March 7, 2016 [Page 11]

Internet-Draft vectors-of-trust September 2015

6.2. Discovery

 The IdP MAY list all of its available trustmarks as part of its

 discovery document, such as the OpenID Connect Discovery server

 configuration document. Trustmarks are listed in the trustmarks

 element which contains a single JSON [RFC7159] object. The keys of

 this JSON object are trustmark provider issuer URLs and the values of

 this object are the corresponding trustmarks for this IdP.

{

 "trustmark": {

 "https://trustmark.example.org/": "https://trustmark.example.org/trustmark/idp.example.org/

 }

}

7. Acknowledgements

 The authors would like to thank the members of the Vectors of Trust

 mailing list in the IETF for discussion and feedback on the concept

 and document.

8. IANA Considerations

 This specification creates one registry and registers several values

 into an existing registry.

8.1. Vector Of Trust Components Registry

 The Vector of Trust Components Registry contains the definitions of

 vector components and their associated demarcators.

 o Demarcator Symbol: P

 o Description: Identity proofing

 o Document: [[ this document ]]

 o Demarcator Symbol: C

 o Description: Primary credential usage

 o Document: [[ this document ]]

 o Demarcator Symbol: M

 o Description: Primary credential management

 o Document: [[ this document ]]

Richer & Johansson Expires March 7, 2016 [Page 12]

Internet-Draft vectors-of-trust September 2015

 o Demarcator Symbol: A

 o Description: Assertion presentation

 o Document: [[ this document ]]

8.2. Additions to JWT Claims Registry

 This specification adds the following values to the JWT Claims

 Registry.

 o Claim name: vot

 o Description: Vector of Trust value

 o Document: [[ this document ]]

 o Demarcator Symbol: vtm

 o Description: Vector of Trust Trustmark

 o Document: [[ this document ]]

 o Demarcator Symbol: vtr

 o Description: Vector of Trust Request

 o Document: [[ this document ]]

9. Security Considerations

 The vector of trust value MUST be cryptographically protected in

 transit, using TLS. The vector of trust value MUST be associated

 with a trustmark marker, and the two MUST be carried together in a

 cryptographically bound mechanism such as a signed identity

 assertion.

10. Privacy Considerations

 By design, vector of trust values contain information about a user's

 identity and associations that can be made thereto. Therefore, all

 aspects of a vector of trust contain potentially privacy-sensitive

 information and MUST be guarded as such.

Richer & Johansson Expires March 7, 2016 [Page 13]

Internet-Draft vectors-of-trust September 2015

11. References

11.1. Normative References

 [OpenID] Sakimura, N., Bradley, J., and M. Jones, "OpenID Connect

 Core 1.0", November 2014.

 [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate

 Requirement Levels", BCP 14, RFC 2119,

 DOI 10.17487/RFC2119, March 1997,

 <http://www.rfc-editor.org/info/rfc2119>.

 [RFC7159] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data

 Interchange Format", RFC 7159, DOI 10.17487/RFC7159, March

 2014, <http://www.rfc-editor.org/info/rfc7159>.

11.2. Informative References

 [SP-800-63]

 , , , , , , and , "Electronic Authentication Guideline",

 August 2013.

Appendix A. Document History

 - 01

 o Added IANA registry for components.

 o Added preliminary security considerations and privacy

 considerations.

 o Split "credential binding" into "primary credential usage" and

 "primary credential management".

 - 00

 o Created initial IETF drafted based on strawman proposal discussed

 on VoT list.

 o Split vector component definitions into their own section to allow

 extension and override.

 o Solidified trustmark document definition.

Richer & Johansson Expires March 7, 2016 [Page 14]

Internet-Draft vectors-of-trust September 2015

Appendix B. Example Extension

 To extend the vector component definitions, a specification MUST

 register its contents in the

Authors' Addresses

 Justin Richer (editor)

 Bespoke Engineering

 Email: ietf@justin.richer.org

 Leif Johansson

 Swedish University Network

 Thulegatan 11

 Stockholm

 Sweden

 Email: leifj@sunet.se

 URI: http://www.sunet.se

Richer & Johansson Expires March 7, 2016 [Page 15]