

DOTS  
Internet-Draft  
Intended status: Standards Track  
Expires: May 3, 2017

R. Moskowitz  
L. Xia  
Huawei  
D. Migault  
Ericsson  
A. Mortensen  
Arbor Networks, Inc.  
October 30, 2016

Strong Identities for DOTS Agents  
draft-moskowitz-dots-identities-00.txt

Abstract

DOTS communications are machine-to-machine oriented communications. In addition DOTS agents are expected to end up in a large number of entities. As a result, in addition to secure, the naming scheme to identify all DOTS agents must be scalable. For these reasons this document recommends the use of cryptographic identifiers or strong Identities as opposed to human readable identifiers for example.

This document proposes two forms of strong Identities for the registration and operation of DOTS Agents. One is 802.1AR LDevID [[Std-802.1AR-2009](#)] X.509 certificates. The other is raw public keys as in HIP [[RFC7401](#)] or TLS/DTLS Raw Public Keys [[RFC7250](#)].

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 May 3, 2017.

Internet-Draft

DOTS Identities

October 2016

## Copyright Notice

Copyright (c) 2016 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 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

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	X.509 LDevID . . . . .	<a href="#">3</a>
<a href="#">1.2.</a>	Raw Public Key . . . . .	<a href="#">3</a>
<a href="#">2.</a>	Terms and Definitions . . . . .	<a href="#">4</a>
<a href="#">2.1.</a>	Requirements Terminology . . . . .	<a href="#">4</a>
<a href="#">2.2.</a>	Definitions . . . . .	<a href="#">4</a>
<a href="#">3.</a>	Problem Space . . . . .	<a href="#">5</a>
<a href="#">3.1.</a>	Trusted Identities . . . . .	<a href="#">5</a>
<a href="#">3.2.</a>	Managing the scope of Trust . . . . .	<a href="#">5</a>
<a href="#">4.</a>	Effectively Managing Identity Trust . . . . .	<a href="#">5</a>
<a href="#">4.1.</a>	The IEEE 802.1AR Device Identity Certificate Model . . .	<a href="#">5</a>
<a href="#">4.2.</a>	The Raw Public Key Model . . . . .	<a href="#">6</a>
<a href="#">5.</a>	IANA Considerations . . . . .	<a href="#">6</a>
<a href="#">6.</a>	Security Considerations . . . . .	<a href="#">6</a>
<a href="#">7.</a>	Acknowledgments . . . . .	<a href="#">6</a>
<a href="#">8.</a>	References . . . . .	<a href="#">7</a>
<a href="#">8.1.</a>	Normative References . . . . .	<a href="#">7</a>
<a href="#">8.2.</a>	Informative References . . . . .	<a href="#">7</a>
	Authors' Addresses . . . . .	<a href="#">8</a>

[1.](#) Introduction

DOTS communications are machine-to-machine oriented communications. In addition DOTS agents are expected to end up in a large number of entities. As a result, in addition to secure, the naming scheme to identify all DOTS agents must be scalable. For these reasons the

document recommend the use of cryptographic identifiers or strong Identities as opposed to human readable identifiers for example.

Human readable identifiers are very helpful to represent a resource for human. A typical example is the use of First Name and Last Name

which is easier for human beings to remember than a phone number. The same occurs for web sites where FQDNs are easier to remember than the IPv6 addresses. However the human readable representation also comes with some issues.

First human readable identifiers have very little entropy which means that when the number of identifiers grow, collision are likely to happen. The likelihood of identifier collision may be limited at the expense of management complexity whose complexity grows with the number of identifiers. Second, human readable identifiers are only meaningful when used by humans who are only able to handle a limited numbers of identifiers. Third the identifier needs to be securely bound to additional element such as security elements - a public key - or routing elements - an IP address - in order to enable a communication.

As a result, human readable identifiers do not scale to meet the need of DOTS identifiers and the management overhead complexity to make identifiers human readable becomes meaningless in a automated machine to machine environment. A DOTS is intended for machine to machine -like communication, there is no reason for using human readable identifiers. DOTS recommends the use of cryptographic identifiers to avoid an additional and unnecessary cryptographic binding between the identifier and the security material.

This document describes two forms of strong Identities for the registration and operation of DOTS Agents.

### 1.1. X.509 LDevID

The first is the X.509 LDevID defined in 802.1AR [[Std-802.1AR-2009](#)]. The methodology proposed herein expects the DOTS mitigation provider to provide a PKI that will issue LDevID certificates to its customers. This provides a strong "domain of trust" to the identities of its customers. Inter provider trust can be established through any of the multi-PKI trust models in use today.

Customer LDevID registration may be based on an "Owner Certificate", allocated to the device during a NETCONF zerotouch registration [[I-D.ietf-netconf-zerotouch](#)]. Or the IDevID could be used directly in some registration process.

## [1.2.](#) Raw Public Key

The second form of Identity is a Raw Public Key.

One type of Raw Public Key is a HIP [[RFC7401](#)] Host Identity (HI). The customer may use HIP DNS Extension [[RFC8005](#)] to assert its HI to

the DOTS mitigation provider and then use HIP to prove ownership of the HI.

Although nothing prevents HI/HIT to be assigned by the provider, there is currently no mechanisms defined for such provisioning. This might be defined in future work, however, the current use of HI/HIT is that these identifiers are generated by the owner or the agent.

Another type of Raw Public Key is defined in [[RFC7250](#)]. The customer would use the methods defined in DANE [[RFC6698](#)] validate a TLS Raw Public Key.

## [2.](#) Terms and Definitions

### [2.1.](#) Requirements Terminology

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](#)].

### [2.2.](#) Definitions

**DOTS Agents:** Per [[I-D.ietf-dots-requirements](#)], any DOTS-aware software module capable of participating in a DOTS signaling session.

**Host Identity (HI):** The term "HI" is defined in [[RFC7401](#)] as "the public key of the signature algorithm that represents the identity of the host." In HIP, a host proves its identity by creating a

signature with the private key belonging to its HI.

**Initial Secure Device Identifier (IDevID):** The term "IDevID" is defined in [[Std-802.1AR-2009](#)] as "the Secure Device Identifier (DevID) installed on the device by the manufacturer". By example, an IDevID certificate, signed by the manufacturer may encode a manufacturer assigned unique identifier (e.g., serial number) and a public key matching a private key held within a TPM chip embedded within the device.

**Locally Significant Secure Device Identifier (LDevID):** The term "LDevID" is defined in [[Std-802.1AR-2009](#)] as "A Secure Device Identifier credential that is unique in the local administrative domain in which the device is used.". By example, an LDevID certificate, signed by the device owner may encode an owner assigned unique identifier (e.g., installation location) and a public key matching a private key held within a TPM chip embedded within the device.

**Owner Certificate:** The term "owner certificate" is defined in [[I-D.ietf-netconf-zero-touch](#)] as used in this document to represent an X.509 certificate, signed by the device's manufacturer or delegate, that binds an owner identity to the owner's private key, which the owner can subsequently use to sign artifacts.

**TLS Raw Public Key:** The term "Raw Public Key" is defined in [[RFC7250](#)]. So a "TLS Raw Public Key" as used in this document to represent this subset of an X.509 certificate used in the manner specified in [RFC7250](#).

### [3.](#) Problem Space

#### [3.1.](#) Trusted Identities

DOTS is meant to be deployed within the context of a business arrangement between a customer and a DDoS mitigation provider. This relationship is long-lived over a persistent session. This relationship and the data communications can best be managed with trusted identities.

Further, the customer's DDoS mitigation provider may need to enlist

the assistance of a peer provider. A strong trusted identity link from the requesting provider back to the attacked customer would benefit the mitigation process.

### [3.2.](#) Managing the scope of Trust

The web's PKI model is fraught with trust leakage challenges. Why trust a specific certificate just because some CA within the list of CAs that must be trusted has signed the certificate? This leads to independent vetting of each client certificate or applying some rules as to which CA is accepted for what business arrangement and then still maintaining a list of accepted client certificates is needed. This leads to a basic question of what is an X.509 certificate providing to the business agreement that would not be needed to be found out independent from the certificate?

## [4.](#) Effectively Managing Identity Trust

### [4.1.](#) The IEEE 802.1AR Device Identity Certificate Model

IEEE 802.1AR [[Std-802.1AR-2009](#)] defines two important types of X.509 certificates. The IDevID is installed in the device in permanent, secure storage (e.g. a TPM) and is NEVER replaced. This certificate is signed by the manufacturer's CA. Typically, its subjectName contains the device's serial number and other information that uniquely identifies the device.

The IDevID is not appropriate to use as an Identifier for any action other than provisioning another Identifier that is more flexible for general use. This limitation is based, in part, on the permanency of IDevIDs and the potential for a large number of CAs 'owning' those IDevIDs.

The second, more regularly usable, type of certificate is the LDevID. This Locally Significant Secure Device Identifier is expected to be signed by a PKI appropriate to its use. For example, the DDoS mitigation provider can maintain its PKI for the signing and validating the device's LDevID certificate. The methodology for an IDevID to leverage the creation of an LDevID is left to IETF protocols. Originally, this meant using PKIX protocols like CMP [[RFC4210](#)]. Recent work with [[I-D.ietf-netconf-zero-touch](#)] can lead to a trusted lDevID request based on the Owner Certificate.

## [4.2.](#) The Raw Public Key Model

With Raw Public Keys, the trust establishment is left to the provider. Authentication based on a Raw Public Key assumes the peer already has the corresponding identifier. Authentication based on raw keys has been integrated by many protocol such as IKEv2, HIP, and TLS. However, unless the identifier is known by the peer, such protocol end with an unauthenticated communication. Provisioning of the identifier, is usually out of scope of these protocol. The Identifier may be provided out of band, using leap of faith mechanisms. Eventually DNSSEC can also be used to bind the identifier to raw key.

There are some recent developments, like Hierarchical HITs [[I-D.moskowitz-hierarchical-hip](#)] that provide an trusted infrastructure for Raw Public Keys.

## [5.](#) IANA Considerations

TBD

## [6.](#) Security Considerations

TBD

## [7.](#) Acknowledgments

TBD

## [8.](#) References

### [8.1.](#) 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, <<http://www.rfc-editor.org/info/rfc2119>>.

[Std-802.1AR-2009]

IEEE SA-Standards Board, "IEEE Standard for Local and metropolitan area networks - Secure Device Identity", December 2009, <<http://standards.ieee.org/findstds/standard/802.1AR-2009.html>>.

## 8.2. Informative References

[I-D.ietf-dots-requirements]

Mortensen, A., Moskowitz, R., and T. Reddy, "Distributed Denial of Service (DDoS) Open Threat Signaling Requirements", [draft-ietf-dots-requirements-02](#) (work in progress), July 2016.

[I-D.ietf-netconf-zerotouch]

Watsen, K. and M. Abrahamsson, "Zero Touch Provisioning for NETCONF or RESTCONF based Management", [draft-ietf-netconf-zerotouch-09](#) (work in progress), July 2016.

[I-D.moskowitz-hierarchical-hip]

Moskowitz, R. and X. Xu, "Hierarchical HITs for HIPv2", [draft-moskowitz-hierarchical-hip-02](#) (work in progress), October 2016.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", [RFC 4210](#), DOI 10.17487/RFC4210, September 2005, <<http://www.rfc-editor.org/info/rfc4210>>.

[RFC6698] Hoffman, P. and J. Schlyter, "The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA", [RFC 6698](#), DOI 10.17487/RFC6698, August 2012, <<http://www.rfc-editor.org/info/rfc6698>>.



Weiler, S., and T. Kivinen, "Using Raw Public Keys in Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", [RFC 7250](#), DOI 10.17487/RFC7250, June 2014, <<http://www.rfc-editor.org/info/rfc7250>>.

[RFC7401] Moskowitz, R., Ed., Heer, T., Jokela, P., and T. Henderson, "Host Identity Protocol Version 2 (HIPv2)", [RFC 7401](#), DOI 10.17487/RFC7401, April 2015, <<http://www.rfc-editor.org/info/rfc7401>>.

[RFC8005] Laganier, J., "Host Identity Protocol (HIP) Domain Name System (DNS) Extension", [RFC 8005](#), DOI 10.17487/RFC8005, October 2016, <<http://www.rfc-editor.org/info/rfc8005>>.

#### Authors' Addresses

Robert Moskowitz  
Huawei  
Oak Park, MI 48237  
USA

Email: [rgm@labs.htt-consult.com](mailto:rgm@labs.htt-consult.com)

Liang Xia  
Huawei  
No. 101, Software Avenue, Yuhuatai District  
Nanjing  
China

Email: [Frank.xialiang@huawei.com](mailto:Frank.xialiang@huawei.com)

Daniel Migault  
Ericsson  
8400 boulevard Decarie  
Montreal, QC H4P 2N2  
Canada

Phone: +1 514-452-2160  
Email: [daniel.migault@ericsson.com](mailto:daniel.migault@ericsson.com)

Andrew Mortensen  
Arbor Networks, Inc.  
2727 S. State St  
Ann Arbor, MI 48104  
United States

Email: [amortensen@arbor.net](mailto:amortensen@arbor.net)

