NOTICE OF REVIEW PERIOD – BALLOT 210

This Review Notice is sent pursuant to Section 4.1 of the CA/Browser Forum's Intellectual Property Rights Policy (v1.2). This Review Period is for Final Maintenance Guidelines (30 day Review Period). A complete draft of the Draft Guideline that is the subject of this Review Notice is attached.

Date Review Notice Sent:	August 31, 2017
Ballot for Review:	Ballot 210 - Misc. Changes to the Network and Certificate System Security Requirements
Start of Review Period:	Sept. 1, 2017 at 01:00 UTC
End of Review Period:	Oct. 1, 2017 at 01:00 UTC

Please forward any Exclusion Notice relating to Essential Claims to the Chair by email to kirk.hall@entrustdatacard.com before the end of the Review Period. See current version of CA/Browser Forum Intellectual Property Rights Policy for details.

(Optional form of Exclusion Notice is attached)

Ballot 210 - Misc. Changes to the Network and Certificate System Security Requirements

--Motion Begins--

In the Network and Certificate System Security Requirements:

ADD ETSI EN 319 411-1 to first sentence of the Scope and Applicability section so that it reads "These Network and Certificate System Security Requirements (Requirements) apply to all publicly trusted Certification Authorities (CAs) and are adopted with the intent that all such CAs and Delegated Third Parties be audited for conformity with these Requirements as soon as they have been incorporated as mandatory requirements (if not already mandatory requirements) in the root embedding program for any major Internet browsing client and that they be incorporated into the WebTrust Service Principles and Criteria for Certification Authorities, ETSI TS 101 456, ETSI TS 102 042 and ETSI EN 319 411-1 including revisions and implementations thereof, including any audit scheme that purports to determine conformity therewith."

REPLACE section 1.a. with "a. Segment Certificate Systems into networks based on their functional or logical relationship, for example separate physical networks or VLANs;"

REPLACE section 1.b. with "b. Apply equivalent security controls to all systems co-located in the same network with a Certificate System;"

REPLACE "90 days" with "three (3) months" in section 2.g.ii. and 2.j so that they read "ii. For accounts that are accessible from outside a Secure Zone or High Security Zone, require that passwords have at least eight (8) characters, be changed at least every three (3) months, use a combination of at least numeric and alphabetic characters, that are not a dictionary word or on a list of previously disclosed human-generated passwords, and not be one of the user's previous four (4) passwords; and implement account lockout for failed access attempts in accordance with subsection k; OR"

AND

"j. Review all system accounts at least every three (3) months and deactivate any accounts that are no longer necessary for operations;"

REPLACE section 2.m. with "m. Enforce multi-factor OR multi-party authentication for administrator access to Issuing Systems and Certificate Management Systems;"

REPLACE section 2.o. with "o. Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when: (i) the remote connection originates from a device owned or controlled by the CA or Delegated Third Party, (ii) the remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and (iii) the remote connection is made to a designated intermediary device (a) located within the CA's network, (b) secured in accordance with these Requirements, and (c) that mediates the remote connection to the Issuing System."

REPLACE "every 30 days and" with "once a month to" in section 3.e. so that it reads "e. Conduct a human review of application and system logs at least once a month to validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log-integrity-verification functions are operating properly (the CA or Delegated Third Party MAY use an in-house or third-party audit log reduction and analysis tool); and"

REPLACE 4.a. with "a. Implement intrusion detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles to protect Certificate Systems against common network and system threats;"

REPLACE 4.C. with "c. Undergo or perform a Vulnerability Scan (i) within one (1) week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that the CA determines are significant, and (iii) at least every three (3) months, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems;"

REPLACE the definition of Security Support System in the Definitions with "Security Support System: A system used to provide security support functions, which MAY include authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and intrusion detection (Host-based intrusion detection, Network-based intrusion detection)."

Make other editorial changes as indicated at https://github.com/cabforum/documents/pull/64/files and in the attached PDF.

--Motion Ends—

EXCLUSION NOTICE – BALLOT _____

I hereby provide this Exclusion Notice for the Essential Claim(s) listed below:

Ballot Covered by This Exclusion Notice: Ballot: _____

CABF Member Name: _____ (Organization)

Date Exclusion Notice Sent: _____

Exclusion Notice provided by: _____ (Name)

Provide Exclusion Notice to current CA/Browser Forum Chair: Kirk Hall, kirk.hall@entrustdatacard.com Exclusion Notices must be provided by deadline stated in related Review Notice.

(For each Essential Claim covered by this Exclusion Notice, please list "numbered section of the Final Guideline or Final Maintenance Guideline whose implementation makes the excluded claim an Essential Claim for each of the issued patent(s) or pending patent application(s) that a Participant reasonably believes at the time may contain Essential Claims the Participant wishes to exclude from the CAB Forum RF License" and also "make an election, (i) not to grant a license or (ii) to provide a license with all of the requirements of Section 5.1 with the exception of subsection 5.1 f." See IPR Policy Sections 4.2 and 4.3.)

Essential Claim No.	Numbered section(s) of Guideline related to Essential Claim [Sec. 4.3]	Patent number for issued patent, title and application number for pending patent, or copy of patent application unpublished patent applications [Sec. 4.3]	License Grant Election Made [Sec. 4.2]
1.			☐ (i) no license granted ☐ (ii) license granted per Sec. 5.1 except Sec. 5.1.f
2.			☐ (i) no license granted ☐ (ii) license granted per Sec. 5.1 except Sec. 5.1.f
3.			☐ (i) no license granted ☐ (ii) license granted per Sec. 5.1 except Sec. 5.1.f
4.			☐ (i) no license granted ☐ (ii) license granted per Sec. 5.1 except Sec. 5.1.f

(Continue on second page if necessary)

Relevant IPR Policy Excerpts

4.2 Excluding Patents and/or Patent Applications from Royalty Free Licensing Obligations during Review Period.

Except for Essential Claims encompassed by a Participant's Contributions that are actually incorporated into a Final Guideline or Final Maintenance Guideline approved in accordance with the CAB Forum Guideline approval process, Participants may within the Review Period exclude Essential Claims from the CAB Forum RF License. In such case, Participant shall be permitted to either make an election, (i) not to grant a license or (ii) to provide a license with all of the requirements of Section 5.1 with the exception of subsection 5.1 f.

4.3 Conditions and Procedure for Excluding Patents and/or Patent Applications from CAB Forum RF License.

*A Participant seeking to exclude Essential Claims from the CAB Forum RF License in accordance with Section 4.2 must provide written notice of such intent to the CAB Forum Chair ("Exclusion Notice") within the Review Period, and the Exclusion Notice shall be effective upon its receipt by the CAB Forum Chair. The Exclusion Notice shall include identification of the numbered section of the Final Guideline or Final Maintenance Guideline whose implementation makes the excluded claim an Essential Claim for each of the issued patent(s) or pending patent application(s) that a Participant reasonably believes at the time may contain Essential Claims the Participant wishes to exclude from the CAB Forum RF License. For issued patents, the Exclusion Notice shall also include the patent number(s). For pending patent applications, the Exclusion Notice shall also include the title and application number(s). If an issued patent or pending patent application that may contain Essential Claims is not set forth in the Exclusion Notice, such Essential Claims shall continue to be subject to the CAB Forum RF License. For unpublished patent applications, the Exclusion Notice shall also include a copy of the patent application. Exclusion Notices shall be published at https://cabforum.org/ipr-exclusion-notices/. ****

8.1. Essential Claims

*"Essential Claims" shall mean all claims in any patent or patent application in any jurisdiction in the world that would necessarily be infringed by implementation of any Normative Requirement in a Final Guideline or Final Maintenance Guideline. A claim is necessarily infringed hereunder only when it is not possible to avoid infringing it because there is no non-infringing alternative for implementing a Normative Requirement of a Final Guideline or Final Maintenance Guideline. Existence of a non-infringing alternative shall be judged based on the state of the art at the time the guideline is adopted as a Final Guideline or Final Maintenance Guideline. If a Normative Requirement in a Final Guideline or Final Maintenance Guideline may be fulfilled by any of a list of specified alternatives, then for determination of whether a claim is an Essential Claim, each of the specified alternatives should be considered independently as if it were the only method for fulfilling that requirement. ****

8.3. Other Key Definitions **

*c. **"Contribution"** means material, including Draft Guidelines, Draft Guideline text, and modifications to other Contributions, made verbally or in a tangible form of expression (including in electronic media) which is provided by a Participant in the process of developing a Draft Guideline for the purpose of*

*incorporating such material into a Draft Guideline or a Final Guideline or Final Maintenance Guideline. For a verbal contribution to be deemed a Contribution hereunder it must be memorialized within approved meeting minutes of the CAB Forum. ****