|  |  |  |
| --- | --- | --- |
| ITU logo | INTERNATIONAL TELECOMMUNICATION UNION**TELECOMMUNICATIONSTANDARDIZATION SECTOR** | **Digital Currency Global Initiative** |
| **DCGI**-**SA-O-002** |
| **Original: English** |
| **WG(s):** | SA WG | e-meeting, 2 September 2020 |
| **INPUT DOCUMENT** |
| **Source:** | Security Assurance Working Group |
| **Title:** | Summary of the 2nd Security Assurance Working Group e-meeting held on 2 September 2020 |
| **Contact:** | DCGI SecretariatITU | E-mail: dcgi-secretariat@itu.int  |

|  |  |
| --- | --- |
| **Keywords:** | Meeting Summary; security assurance; DCGI |
| **Abstract:** | This document contains the summary record of the 2nd Security Assurance Working Group (SA WG) e-meeting of 2nd September 2020. |

# Opening of meeting & welcome

## The second meeting of the Digital Currency Global Initiative Security & Assurance WG meeting took place online via Mymeetings platform on 2 September 2020 (15:00 – 16:30 CEST).

## The meeting was chaired by Jacques Francoeur, Team Leader (Chairman) of the working group and was assisted by Vijay Mauree and Charlyne Restivo from ITU.

## Some 40 participants attended the meeting remotely. The list of participants is in document [DCGI-SA-I-020](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-020.pdf) (see meeting documents, which can be accessed with ITU TIES or Guest account on the Security & Assurance WG collaboration Sharepoint website: <https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/SitePages/security.aspx>).

## The agenda for the meeting can be found in document [DCGI-SA-I-011-R1](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-011-R1.docx).

## The Chairman indicated that the purpose of the meeting was to provide an overview of the discussions that has taken place on the workplan, working group structure, the digital currency security model, integrating the FG DFC security reports in the work plan and present contributions received for this meeting. It was noted that the following contributions were received for this meeting:

|  |  |  |
| --- | --- | --- |
| * [DCGI-SA-I-013](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-013.docx)
 | Expansion of dimensions for privacy, traceability and transaction cost | Assaf Klinger, Vaulto |
| * [DCGI-SA-I-014](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-014.pdf)
 | FG-DFC report on Protection Assurance for Digital Currencies | DCGI Secretariat |
| * [DCGI-SA-I-015](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-015.pdf)
 | FG-DFC report on Protection Assurance Use Case for a Payment transaction | DCGI Secretariat |
| * [DCGI-SA-I-016](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-016.zip)
 | A Survey of Research on Retail Central Bank Digital Currency | M. Malaika, IMF |
| * [DCGI-SA-I-017](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-017.pptx)
 | Presentation of WG Structure, Terms of Reference, FG DFC Deliverables & WG Activities | Jacques Francoeur, Team Leader |

# Presentation on Working Group Structure and Work Plan (See [DCGI-SA-I-017](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-017.pptx))

## The Chairman presented the Working Group structure and work plan for the short term. The responsibilities for the Vice Team Leaders have been assigned as show in slide 7 of the presentation. During the presentation, Chairman requested team members to contact each Vice Team Leaders to specify or send their contributions.

## According to the work plan the first step will be to consider one digital currency type (eg retail central bank digital currency) and investigate the issuance, distribution and payment use case and conduct a business impact analysis to specify the security requirements for each use case.

## The Chairman mentioned that the mapping of threats and vulnerabilities for applications that are based on DLT will make use of the work in ITU-T Study Group 17, Recommendation ITU-T X.1401 and X.1402 which already defines the threat vectors for DLT based systems from a protocol, network and data layer perspective.

## It was noted that the security of the digital wallet would also be in the scope of the work when considering the payment use case.

# Vice Team Leader Briefings

## Paul Lloyd mentioned that in his workstream the focus will be on the cryptography technique used in digital currency and how to make them quantum safe. He invited members to contact him if they would like to send any contributions on this topic for the next meeting.

## Mitch Cohen mentioned that he will be working closely with the Chairman in defining the security use cases (ie issuance, distribution and payment). The example of eCurrency and how security is addressed in the platform will be considered. He invited others who could contribute on the security use cases of other digital currency platforms to send their contributions for the next meeting.

## Majid Malaika made a presentation (see doc [DCGI-SA-I-016](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-016.zip) and presentation slides in [DCGI-SA-I-019](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/_layouts/15/WopiFrame.aspx?sourcedoc=%7BEC542AD0-D051-4ABF-9B6D-421CC5359508%7D&file=DCGI-SA-I-019.pptx&action=default)) on the operational design and cybersecurity risks for retail Central Bank Digital Currency based on a study from the IMF. The study covered the examples of retail CBDC pilot projects in Bahamas, Sweden, Uruguay and ECCB). The ability for retail CBDC to support offline transactions is an important requirement from Central Banks. Some of the key challenges for cybersecurity risks mentioned during the presentation were:

* + Insider threats
	+ Shared vulnerabilities with cloud providers
	+ Hardware vulnerabilities (Spectre and Meltdown)
	+ APIs use
	+ Encryption keys
	+ Anonymity levels compared to information needed to be kept for AML/CFT requirements compliance

## Majid will be focusing mainly on the security design considerations for CBDCs.

# Presentation of Contribution [DCGI-SA-I-013](https://extranet.itu.int/sites/itu-t/initiatives/dcgi/wg/input_security/DCGI-SA-I-013.docx)

## Since Assaf Klinger had to leave the meeting, Vijay Mauree, ITU Secretariat, read the message sent by him with regards to his contribution:

*The contribution states that traceability, privacy and transaction cost are not scalar. For each digital currency type, the level of traceability, privacy and transaction cost differ depending on the stakeholder in the digital currency ecosystem. The suggestion is to represent the level of traceability, privacy, and transaction cost as a graph with each vertex representing the level of traceability, privacy and transaction cost.*

## The contribution was noted and since Mr Assaf Klinger was not present for questions, it was requested that he submits a more detailed paper at future meeting to explain his contribution further.

# Liaisons to other groups

## The Chairman invited Ed Scheidt, ISO Convener for Digital Currency Security to share some of the work ongoing in ISO on this topic. Ed mentioned that ISO is doing work on security for digital currency and will be soon releasing a document in this area which could be shared with the group if we have a liaison agreed with them.

## Other groups of interest for liaisons were NIST and ETSI working group on digital currency.

## The ITU Secretariat will contact these institutions to request them to nominate a focal point for participating in the Security Working Group.

# Next meeting

The next meeting the SA WG will take place on **6th October, at 15h00 (CEST).**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_