



**WSIS
FORUM 2026**

**6-10 July 2026
Geneva, Switzerland**

Session Outcome Document

Building Trust and Protection for Essential Digital Infrastructure: The Digital Emblem Project From Standards to Deployment

International Committee of the Red Cross

11:15 – 12:00, Friday July 8th

<https://www.itu.int/net4/wsis/forum/2026/en/Agenda/Session/436>

Key Issues discussed:

- The growing dependence of medical services, humanitarian organizations and other essential civilian services on digital infrastructure—and the serious human consequences that can result when this infrastructure is disrupted during armed conflict.
- The concept of a digital emblem as a technical means of identifying digital infrastructure associated with entities and activities protected under international humanitarian law, without creating new legal protections or altering the applicable rules of IHL.
- The progress made in moving the Digital Emblem Project from an initial concept towards operational implementation, including the development and demonstration of a prototype technical architecture.
- The importance of ensuring that a digital emblem can be issued, displayed and verified in a manner that is trustworthy, secure, decentralized and compatible with the operational realities of protected entities and potential verifiers.
- The role of open and inclusive technical standardization, including ongoing work within the Internet Engineering Task Force and engagement with the International Telecommunication Union, in promoting interoperability and global adoption.
- The need for continued testing with medical services, National Red Cross and Red Crescent Societies, humanitarian organizations, cybersecurity practitioners and other relevant stakeholders to determine whether proposed solutions are feasible, understandable and compatible with existing systems.

Key Outcomes of the session

- Participants gained a clearer understanding of how the Digital Emblem Project seeks to translate existing IHL protections into a recognizable and verifiable technical signal for the digital environment.
- The discussion confirmed that technical feasibility alone is insufficient: effective implementation will also depend on legal clarity, trusted authorization processes, interoperability, operational testing and recognition by those expected to verify the emblem.
- The session highlighted the importance of designing the digital emblem through a genuinely multistakeholder process involving States, protected entities, humanitarian organizations, technical experts, standards bodies, cybersecurity practitioners, and industry.

Key Recommendations and Forward-Looking Actions

- Support the development of open, interoperable and globally accessible technical standards for the digital emblem through inclusive international standards processes; important to ensure that this process includes diverse stakeholders from across regions and professions.
- Expand structured testing in realistic operational environments, particularly with medical services, National Red Cross and Red Crescent Societies and other eligible humanitarian actors, while separately engaging cyber operators and other potential verifiers.