

## PSCC Subcommittee SG 14 Meeting Minutes

Designation: SG 14		Name: Study Group for the use of HTTP and TLS for devices in Electric Power Systems			
Meeting Location: Virtual		Meeting Time: 11.30 CST	Meeting Date: 2021/09/20	Minutes Revised: [yyyy/mm/dd]	Minutes Approved: [2022/10/01]
PAR Output: N/A	PAR Output:	PAR Approval Date:	PAR Expiration Date:	Target Sponsor Ballot Date:	Target Completion Date:
Presiding Officer: Shashi Sastry Chair, Colin Gordon Vice-chair			Recorded by: Colin Gordon	Draft Number: 1.0	
Attendance:					
Name		Affiliation		Phone (P) / Web (W) / Local (L)	M/CM/G
Colin Gordon	Schweitzer Engineering Labs	W	M		
Craig Preuss	Black & Veatch	W	M		
Deryk Yuill	iS5 Communications	W	M		
Dennis Holstein	OPUS Consulting Group	W	M		
Eric Thibodeau	Hydro Quebec	W	M		
Gayle Nelms	Schweitzer Engineering Labs	W	M		
Herbert Falk	UTB Consulting	W	M		
James Formea	Eaton	W	M		
Joe Xavier	ABB	W	M		
Jackie Willson	Ameren	W	M		
Jeremy Slimmer	Cybirical	W	M		
Jeff Pack	Synapt	W	M		
Karen Leggett Wyszczelski	Schweitzer Engineering Labs	W	M		
Mario Capuozzo (Doble)	Doble	W	M		
Nathan Wallace	Cybirical	W	M		
Scott Mix	PNNL	W	M		
Steven Kunsman	Hitachi ABB	W	M		
Shashi Sastry	Hitachi ABB	W	M		
Steven Blair	Synapt	W	M		
Tony Bell	Schweitzer Engineering Labs	W	M		
Wayne Pawley	Sisco	W	M		
M: Member CM: Corresponding Member G: Guest					

Item no.	Notes	Action by
<b>CALL TO ORDER</b>	Meeting was called to order at 11.35 CST	Shashi
<b>INTRODUCTIONS AND QUORUM</b>	Total 23 attendees; Brief intro by Shashi and Colin	Shashi & Colin
<b>CHAIR'S REMARKS</b>	Introduced the study group and mentioned title change or SG14 (TLS only). New Chair and Vice Chair introductions and overview of the agenda.	All

Item no.	Notes	Action by
<b>AGENDA</b>	<ul style="list-style-type: none"> <li>▪ Brief introductions: Shashi and Colin</li> <li>▪ Approval of the previous minutes from May 2021</li> <li>▪ Review mission of the SG S14</li> <li>▪ Proposed move to a Task Force</li> <li>▪ Discussion and next steps</li> <li>▪ Introduction to the iMeet central collaboration space</li> </ul>	ALL
<b>APPROVAL OF PREVIOUS MINUTES</b>	Approved.	ALL
<b>[AGENDA ITEM 1]</b>	<p>Outcome of the last meeting:</p> <ul style="list-style-type: none"> <li>▪ SG S14 met on Monday May 3, 2021 @11:30 CST with 29 participants</li> <li>▪ Reviewed the January meeting discussion with focus on moving SG S14 to a Task Force</li> <li>▪ The SG discussed whether to move into a WG with the intent to fast track a guide or recommend practice vs. TF to produce a report</li> <li>▪ <b>Conclusion:</b> Move S14 into TF with focus on a fast-track report allowing NERC and IEC to progress on their standards effort related to encryption and end-to-end authentication</li> <li>▪ Developed the proposed TF Assignment</li> <li>▪ SG approved the motion to request S0 SC approval to move S14 into a Task Force. The request has been made to S0 officer to discuss the below proposal under SC New Items.</li> </ul>	Steven Kunsman
<b>[DISCUSSION ITEM 1]</b>	<p>Re-review of SG S14 purpose</p> <ul style="list-style-type: none"> <li>▪ Re-review of TF S14 assignment and mission (focus) for the task force (if approved as task force)</li> <li>▪ Are we trying to work with TLS 1.3 today or trying to improve it? (Herb)</li> <li>▪ Both TLS 1.2 and 1.3 as changes have happened (null cipher suite)</li> </ul>	Shashi, Herb, Colin
<b>[DISCUSSION ITEM 2]</b>	<ul style="list-style-type: none"> <li>▪ What happens when certificate expires (re-authentication example)? (Herb)</li> <li>▪ Certificate expiration and revocation are two different events</li> <li>▪ Key management (rotation and lifetime), long-time persistent connections and key lifetimes are an important consideration (Herb, Steven)</li> </ul>	Herb, Steven
<b>[DISCUSSION ITEM 3]</b>	<ul style="list-style-type: none"> <li>▪ We can create an outline of the draft document and include section for topics we want to discuss (Shashi)</li> <li>▪ Edge inspection and how this works – breaks mutual authentication on an end-to-end basis (Herb)</li> <li>▪ Use of pre-shared keys or secrets may be the way to make edge inspection work end-to-end (Colin)</li> </ul>	Shashi, Herb, Colin
<b>[DISCUSSION ITEM 4]</b>	<ul style="list-style-type: none"> <li>▪ Share a copy of the draft of 62351-9 CDV – OSCP is used, renegotiation for symmetric keys (Herb)</li> <li>▪ How do we request other documents? (Colin)</li> <li>▪ Question to Herb - include changes between TLS 1.2 and TLS 1.3? (Steven, Colin)</li> <li>▪ We should include 1.2 because the report should include systems and devices which are available today (James)</li> </ul>	Herb, Colin, Steven, James

Item no.	Notes	Action by
<b>[DISCUSSION ITEM 5]</b>	<ul style="list-style-type: none"> <li>▪ Are there any compliance or regulatory requirements to move adopt 1.3? (Shashi)</li> <li>▪ UCA will compliance test TLS 1.3 and not 1.2. What will the industry accept – TLS 1.2 should be included from that point of view (Herb)</li> <li>▪ Information on the delta (1.2 and 1.3) should be evaluated. UCA won't outright forbid 1.2. It won't declare it non-conformant. (Steven)</li> <li>▪ What about mixing 1.2 and 1.3 devices? Interoperability. What concerns should we have for introducing 1.3 in a 1.2 system? (Herb)</li> <li>▪ Is TLS 1.0, 1.1 deprecated? (Steven) Discussion on deprecation to be explored further</li> <li>▪ Reference to RFC 8996</li> <li>▪ Focus on the comparison of TLS 1.2 and 1.3, and the pros and cons of each version (Shashi)</li> </ul>	Shashi, Herb, Steven, James
<b>ACTION</b>	<ul style="list-style-type: none"> <li>▪ Include an official assignment for the task force and timeline</li> <li>▪ Full report September 2023, with usable draft available September 2022.</li> </ul>	Shashi Sastry, Colin, Craig
<b>CLOSING REMARKS/FINAL CONCLUSION</b>	<p>Email participant list for contribution. Add members to the iMeet collaboration space</p>	Shashi Sastry
<b>ITEMS REPORTED OUT OF EXECUTIVE SESSION</b>		
<b>TIME OF FINAL ADJOURNMENT</b>	12.33 p.m. CST	
<b>NEXT VIRTUAL MEETINGS</b>	January 2022	
<b>FUTURE MEETING ROOM REQUIREMENTS</b>	<p>[Room Size][Projector][Conflicts] Room for 30, Webex, Computer Projector (when we meet in person)</p>	