xMatters Email Security

by Robert Hawk and Adam Serediuk

xMatters Information Assurance team
Wednesday 06 February 2019

Introduction

xMatters enhances collaboration by relaying relevant data between key systems while engaging the right people to proactively resolve issues. This integration-driven approach enables enterprises to avoid costly incidents, prevent outages, and streamline DevOps processes. For any given situation, xMatters automatically identifies the appropriate individuals or group and empowers them to take action. With over 200 integrations across a wide range of IT tools, xMatters is used by individual teams for day-to-day tasks, and across thousands of teams at Global 2000 companies working together at enterprise scale. Founded in 2000, xMatters is headquartered in San Ramon, CA, with additional offices worldwide.

xMatters specializes in tool chain integration and communications over multiple devices that provide voice, Short Message System (SMS) text, electronic mail (email) and xMatters Mobile Application for Smart Devices running Apple iOS and Google Android. xMatters communications management is used for Business Continuity Management (BCM), Information Technology Management (ITM) and general notification. xMatters communications management service is defined as Software as a Service (SaaS) Private Cloud per the National Institute of Standards and Technology (NIST) Special Publications 800-145 – The NIST Definition of Cloud Computing.

In regard to the delivery of emergency communications xMatters uses email as one of the delivery methods. This document describes the email security mechanisms.

xMatters Email Transport Security

Simple Mail Transfer Protocol (SMTP) based on Internet Engineering Task Force (IETF) Request for Comment (RFC) 821, 974, 1869, and 2128. xMatters email servers will attempt to negotiate a Transport Layer Security (TLS) version 1.2 tunnel, however if the security negotiation fails then the email will be sent in clear text as the business case for email is such that email may be sent protected by cryptographic controls as per the RFC standard.

xMatters Email Security

Three specific email security technologies specified by the Internet Engineering Task Force (IETF) Request for Comment (RFC) documents in regard to email security used by xMatters are:

- DomainKeys Identified Mail (DKIM)
  IETF RFC 6376
  Permits a person, role, or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message.

  xMatters uses 2048 bit signing DomainKeys Identified Mail (DKIM) for authentication to verify the origin of email.

- Sender Policy Framework (SPF)
  IETF RFC 7208
  Email on the Internet can be forged in a number of ways. In particular, existing protocols place no restriction on what a sending host can use as the "MAIL FROM" of a message or the domain given on the SMTP HELO/EHLO commands. The Sender Policy Framework (SPF) protocol, whereby ADministrative Management Domains (ADMDs) can explicitly authorize the hosts that are allowed to use their domain names, and a receiving host can check such authorization.

  xMatters configuration for Sender Policy Framework (SPF) hard-fail mechanisms, to prevent email spoofing.

- Domain-based Message Authentication, Reporting and Conformance (DMARC)
  IETF RFC 7489
  Is a scalable mechanism by which a mail-originating organization can express domain-level policies and preferences for message validation, disposition, and reporting, that a mail-receiving organization can use to improve mail handling.

  xMatters configuration for Domain-based Message Authentication, Reporting and Conformance (DMARC) validation, to detect and prevent email spoofing, combined with SPF and DKIM with the reject policy set.

End of Document

The rest of this page is left blank intentionally