From ISDN to IP

As services begin to converge to use the Internet, and its associated IP, there will be an increasing need for awareness by sites of security issues for IP-based voice, video and data exchanges.

In an IP world, the point-to-point security and relative privacy of an H.320 ISDN videoconferencing system is no longer present. Where ISDN video and audio calls would be circuit switched across a private provider network, IP-based H.323 calls transit an open network – the Internet – and the devices used for the conferencing, i.e. the end systems and H.323 components such as gatekeepers or MCUs, may all be reachable from the public Internet. If they are present on the Internet, there are associated risks.

In the context of IP-based communications within Janet, communications would flow only over the regional MANs and the Janet backbone, which to an outsider is in effect a ‘private’ network. Thus H.323 sessions where only Janet sites participate would generally be seen as relatively private. The introduction of a non-Janet site to a multi-party conference would raise the question as to which networks the traffic transits, but such concerns would be equally applicable to e-mail as they are to H.323.

This guide is not directly applicable to ISDN conferencing users, but such users should bear in mind that if they join a conference that has a gateway to one or more H.323 conference participants, while their point-to-point dial-in connection to the gateway device is relatively private, data relayed into the H.323 domain may not be as secure.

H.323 is clearly an important protocol for videoconferencing in the Janet community for the foreseeable future. H.323 videoconferencing is already deployed in studio systems, for example in the Welsh Video Network [WVN], and in an IP Videoconferencing pilot that was operated across Janet during 2002.

In the context of high-quality videoconferencing deployments, the end systems are studiobased ones. Until recently most desktop systems were not capable of delivering the quality of videoconferencing experience that (more expensive) studio systems can deliver. However, the quality of desktop systems is improving rapidly. The notes in this guide are largely aimed at assisting the deployment of dedicated studio-based systems, but desktop H.323 users should also be aware of the security issues.

While the security principles apply to all H.323 systems, references to considerations for studio-based systems are made throughout the document.

The Janet IP Videoconferencing Service (JVCS-IP)

The IP Videoconferencing service includes a central gatekeeper and MCUs deployed at Core

Points of Presence (C-PoPs) on the Janet backbone. Based on experience of early trials, it has been determined that MCUs should not be used in a cascaded mode with other MCUs. Thus MCU components are not recommended at the local site; conferences should use the centrally provided MCUs, so we only discuss MCUs very briefly in this document.

As a result, studio systems booked for JVCS-IP H.323 videoconferences will communicate directly with the central MCUs that will initiate all connections out to the studio systems. This ‘call out’ model assists in simplifying some security and support issues, but by no means all of them.

Note that in the JVCS-IP, it is considered preferable for sites to deploy their own gatekeeper, so they can control their local security policy. However, there will be a Janet gatekeeper available for sites that do not have their own gatekeeper and for guest venues not located at a Janet site. Where sites choose to deploy their own MCU for site conferencing, this should not be used on videoconferences run over the JVCS-IP, since the central service does not support cascaded MCUs.

The H.323 standards support both voice and videoconferencing. In this document we refer to videoconferencing.
