

Make your agent ask better.

Hushh gives external agents a consent-first route to relevant information: discover what is available, ask for one narrow scope in plain language, wait for the person, then receive an encrypted export only after approval.

01 Discover Search the person’s live scope catalog. Never hard-code a broad profile request.	02 Request State one returned scope and a human-readable purpose.	03 Approve The person decides in Hushh—not in a hidden agent workflow.	04 Confirm Check the request state. A pending request is not access.	05 Retrieve Use the approved grant to receive the encrypted, bounded export.
---	--	---	---	---

REMOTE MCP Build into the tools people already use. Remote MCP uses a bare endpoint and bearer or OAuth app authentication. Credentials stay out of URLs; personal data still needs a separate consent decision.	ENTERPRISE LANE Connect systems deliberately. An approved export does not authorize a CRM mutation. Read, create, and update require a signed-in owner, typed intent, confirmation, binding, idempotency, and readback. Delete is blocked in v1.
---	---

 Developer workspace hushh.ai/developers	 Open-source research github.com/hushh-labs/hushh-research	 Developer community hushh.ai/discord
--	---	--

FIVE TOOLS, ONE LIFECYCLE Search user scopes · request consent · check consent status · get encrypted scoped export. A compatibility context tool exists, but it is not the normal path.	AUTHENTICATE THE APP. ASK THE PERSON. Bearer or PKCE lets a developer app connect. It never gives that app automatic access to someone’s personal information.	KEEP THE SECRET OUT OF THE MODEL. No query-token URLs. No plaintext fallback. Connector private keys and ciphertext do not belong in a prompt, log, or tool description.
--	--	--

THE CONTRACT A good integration asks for the smallest thing it needs, makes the person’s choice visible, and leaves a trail that can be checked later.
--